MY ENDPOINT PROTECTOR

Version 4.4.0.3

User Manual

COSOSYS

Table of Contents

1. Introduction 1
1.1. What is My Endpoint Protector? 2
1.2. Main Features 2
1.3. Controlled Device Types / Ports 3
1.4. Windows and Mac OS X Client Support 5
1.5. Conclusions 5
2. Cloud Server Functionality 6
2.1. Accessing My Endpoint Protector Online Administration and Reporting Tool 6
2.1.1. Sign-Up 6
2.1.2. Login 7
2.1.3. Forgot your Password 7
2.1.4. Logout 7
2.2. Online Administration and Reporting Tool 7
3. My EPP Client System Requirements 10
4. Client Installation 11
5. Device Control 13
5.1. Global Rights 13
5.2. Effective Rights 13
5.2.1. Effective Rights Endpoints 13
5.2.2. Effective Rights Devices 14
5.3. Global Settings 15
5.4. Devices 15
5.5. Device Rights Functionality 16
5.5.1. Give / Deny Access to Devices 17
5.5.2. Enable Device Read-Only Access 19
5.5.3. TrustedDevice Level 1 to Level 4 19
5.5.4. WiFi - Block if wired network is present 19
5.6. Computers 19
5.6.1. Computer Self Registration 20

5.7. Computer Rights 20
5.8. Computer Settings 21
5.9. Modes for Computers and Groups 22
5.9.1. Transparent Mode 22
5.9.2. Stealth Mode 23
5.9.3. Panic Mode 23
5.9.4. Hidden Icon Mode 23
5.9.5. Silent Mode 23
5.10. Users 24
5.11. User Rights 25
5.12. Groups 26
5.13. Group Rights 27
5.14. Group Settings 28
5.15. Custom Classes 28
6. Content Aware Protection 31
6.1. Content Aware Policies 32
6.1.1. Priorities for Content Aware Policies 33
6.1.2. How Content Aware Policies Work 34
6.1.3. Types of Content Aware Policies 35
6.1.4. Setting up Content Aware Policies 36
6.2. Custom Content Dictionaries 41
6.3. Content Aware URL Whitelists 42
6.4. Content Aware Domain Whitelists 42
6.5. Content Aware Regex (Regular Expressions) 43
6.6. How Content Aware Protection works for monitored Applications / Online Services 44
7. Offline Temporary Password 46
7.1. Device Offline Temporary Password 46
7.2. Computer Offline Temporary Password 48
7.3. Content Aware Protection Offline Temporary Password 48
7.4. Offline Device, Computer and Content Aware Protection Authorization 49

7.5. Setting the Administrator Contact Information 50
8. Reports and Analysis 51
8.1. Content Aware Report 51
8.2. Admin Actions 52
8.3. Online Computers 53
8.4. Online Users 53
8.5. Online Devices 54
8.6. Computer History 55
8.7. User History 55
8.8. Device History 56
9. Alerts 57
9.1. Define Alerts 59
9.2. Alerts History 60
9.3. Define Content Aware Alerts 61
9.4. Content Aware Alerts History 62
9.5. Define MDM Alerts 62
9.6. MDM Alerts History 63
10. Downloads 64
10.1. Installation Files & Enrollment 64
10.2. EasyLock Encryption Software 64
11. My Account 66
11.1. Profile Details 66
11.2. Unique ID 66
11.3. My Subscriptions 67
11.3.1. Trial license 68
11.3.2. Appetizer license 68
11.4. Get a Subscription 68
11.5. Client Uninstall Protection 69
12. My EPP App for iPhone and iPad 70
13. Enforced Encryption with TrustedDevices 71

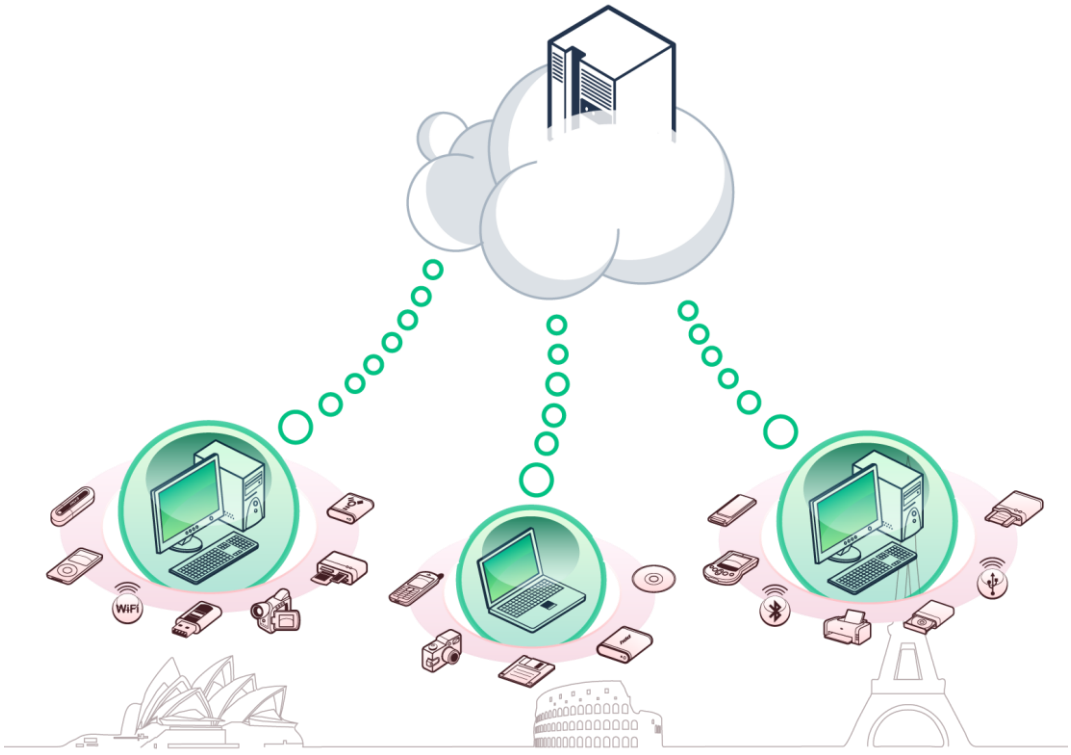
13.1. How a Level 1 TrustedDevice Works 72
13.2. EasyLock Software for TrustedDevices Level 1 73
14. My Endpoint Protector Client 74
14.1. My Endpoint Protector Client Security 74
14.2. Client Notifications (Agent) 74
14.3. Offline Functionality for My Endpoint Protector Client 75
14.4. DHCP / Manual IP address 75
14.5. Client Removal 75
14.5.1. Client Removal on Windows OS 75
14.5.2. Client removal on MAC OS X 76
15. Terms and Definitions 77
15.1. Server Related 77
15.2. Client Related 77
16. Endpoint Protector Product Family 80
17. Support 81
18. Important Notice / Disclaimer 82

1. Introduction

Portable storage devices such as USB flash drives, digital cameras and MP3 players/iPods are virtually everywhere and are connected to a PC via plug and play within seconds.

With virtually every PC having easily accessible USB ports, the theft of data or accidental loss of data is for individuals a mere child's play.

Data theft or infecting the company's network through a simple connection is easy and doesn't take more than a minute. Network administrators had little chance to prevent this from happening or to catch the responsible user(s). This was the hard reality until now.



1.1. What is My Endpoint Protector?

My Endpoint Protector SaaS (Endpoint Security-as-a-Service) provides device control and data loss prevention to customers who don't have the time and resources to manage their own on premise endpoint security solution.

My Endpoint Protector allows individuals and companies of all sizes to manage all their endpoints from one centralized online console, be it Desktops, Notebooks or Netbooks, used in the office, at home or on the road. My Endpoint Protector is eliminating the risks of data loss and data theft that are posed by portable devices like USB Flash Drives.

Controlling ports and devices through a server in the cloud is the best solution to centrally manage one or more PCs or MACs without having to become an expert in installing and managing servers.

1.2. Main Features

Your confidential sensitive data is only as safe as your endpoints are. My Endpoint Protector offers powerful features in order to control, monitor and enforce network and endpoint security.

1. Centrally manage your endpoint / device use from anywhere

2. No server setup (hardware, licenses or maintenance)

3. Enterprise class endpoint security for every size company

4. Manage one or hundreds of PC or MAC endpoints from one online place

5. Every PC user can set it up. No experienced Admin needed

6. Setup in minutes

7. Works with any PC or MAC that has an internet connection

Centralized web based Device Management / Dashboard

Network administrators have the ability to centrally manage and authorize the use of devices. The My Endpoint Protector Dashboard is designed to meet the needs of both management and security staff and offer access to real-time information, charts and reports about organization wide controlled device and data transfer activity. All in an integrated single view and web based Administration and Reporting Tool.

Enforcement of your Device use Policy

Simple device management policies with customizable templates help define User Group permissions to allow for an efficient enforcement and maintenance of your latest security policies across your network. Enforce internal device use policies with ease. Comply with government regulations, industry standards and IT governance in regard to data breach prevention and management has just become easier.

Content Aware Protection

Separate module, which allows creating and enforcing strong content aware policies for a better control of what data leaves the company network via any removable media or the Internet.

Reporting and Analysis

My Endpoint Protector offers powerful reporting and analysis tools that lets you analyze all activity (e.g. devices connected, files transferred, etc) at the endpoint.

Network "Offline" Mode to Support Your Field Employees

"Offline Temporary Password" to allow limited time access to a specific device when the client computer is disconnected from the network.

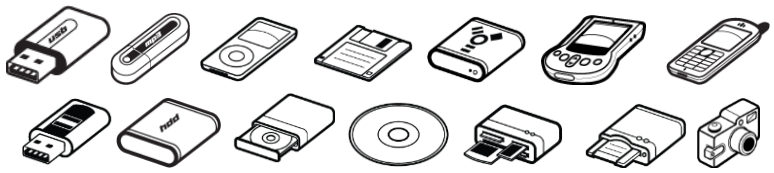
Protected PCs that are temporary or frequently disconnected from the network like laptops stay protected based on the last locally saved policy. All notifications are transmitted at the next network connection.

Enforced Encryption / TrustedDevices

Using Enforced Encryption with TrustedDevices gives the security that all endpoint devices are not only authorized and controlled, but also protecting sensitive and confidential data in transit. With the use of EasyLock to enforce encryption, all data saved is encrypted while in transit.

1.3. Controlled Device Types / Ports

My Endpoint Protector supports a wide range of device types which represent key sources of security breaches. These devices can be authorized which makes it possible for the users to view, create or modify their content and for administrators to view the data transferred to and from the authorized devices.



- Removable Storage Devices
- Normal USB Flash Drives, U3 and Autorun Drives, Disk on Key, etc.
- USB 1.1, USB 2.0, USB 3.0
- Wireless USB
- LPT/Parallel ports
  By controlling the Parallel ports of a PC using My Endpoint Protector, the network administrator can deny or allow users access to storage devices connected to these ports.
  * APPLIES ONLY TO STORAGE DEVICES
- Floppy disk drives
  Access to floppy disk drives can be managed through My Endpoint Protector and can be turned on/off completely.
- Memory Cards - SD Cards, MMC Cards, and Compact Flash Cards, etc.
  These devices can be enabled / disabled via My Endpoint Protector.
- Card Readers - internal and external
  These devices can be enabled / disabled via My Endpoint Protector.
- CD/DVD-Player/Burner - internal and external
  These devices can be enabled / disabled via My Endpoint Protector.
- Digital Cameras
  These devices can be enabled / disabled via My Endpoint Protector.
- Smartphones / Handhelds / PDAs
  This category includes Nokia N-Series, Blackberry, and Windows CE compatible devices, Windows Mobile devices, etc.
- iPods / iPhones / iPads
  These devices can be enabled / disabled via My Endpoint Protector.
- MP3 Player / Media Player Devices
  These devices can be enabled / disabled via My Endpoint Protector.

- External HDDs / portable hard disks
  These devices can be enabled / disabled via My Endpoint Protector.

- FireWire Devices
  These devices can be enabled / disabled via My Endpoint Protector.

- PCMCIA Devices
  These devices can be enabled / disabled via My Endpoint Protector.

- Biometric Devices
  These devices can be enabled / disabled via My Endpoint Protector.

- Bluetooth
  These devices can be enabled / disabled via My Endpoint Protector.

- Printers
  Applies to serial, USB and LTP connection methods. These devices can be enabled / disabled via My Endpoint Protector.

1.4. Windows and Mac OS X Client Support

All features in My Endpoint Protector are available for Windows Clients. The support for Mac OS X Clients is in some ways limited, but all core security features are also supported for Mac OS X. We do our best to not only have My Endpoint Protector as the best device control and endpoint security solution for Windows but also for Mac OS. Thank you for your support and understanding.

1.5. Conclusions

As information theft and proprietary data leakage are a reality of today's business world, effectively preventing all possible security breaches is becoming an ultimate concern for enterprise security experts. Endpoint security comes to complete your existing security policies, aiming to render it full proof.

As new circumvention and data compromising techniques come to diminish the benefits of new devices and gadgets, My Endpoint Protector secures your company's technologically enabled mobility. Thus, by easily protecting all exposed endpoints from inbound and outbound threats, you can enjoy enhanced portability, efficiency and productivity.

As it enables your employees to use devices you have already invested in and it protects your company from losses generated by attacks from outside and within, all financial costs entailed by implementing My Endpoint Protector, such as purchase, implementation and usage training expenses, are fully justified by the yielded return on investment.

2. Cloud Server Functionality

The functionality of the My Endpoint Protector is designed to be around several physical entities:

- Computers (PCs or MACs with My Endpoint Protector client installed)
- Devices (the devices, which are currently supported by My Endpoint Protector. e.g.: USB devices, digital photo cameras, USB memory cards etc.)
- The cloud/server side of My Endpoint Protector is the Administration and Reporting Tool. It is responsible for centrally managing devices, computers, users, groups and their behavior together

2.1. Accessing My Endpoint Protector Online Administration and Reporting Tool

To access the online Administration and Reporting Tool, simply open a browser and enter the My Endpoint address.

https://my.endpointprotector.com

Here you will need to enter your username and password.

If you have not already done so, please provide a user name and sign-up for My Endpoint Protector to receive your login credentials.

2.1.1. Sign-Up

To create a My Endpoint Protector account, please choose a username and password and follow the steps in the sign-up wizard. To finish the sign-up process, you need to confirm your e-mail address. For this please click the confirmation link in the e-mail that you will receive.

2.1.2. Login

To login to your My Endpoint Protector Account you need to enter your username and password here https://my.endpointprotector.com

2.1.3. Forgot your Password

In case you forgot your username and / or password or both, please provide your e-mail address that you used in the registration process after clicking "Forgot your password?". Then your password will be reset and a new password will be sent to you.

2.1.4. Logout

To Logout of your My Endpoint Protector Account simply click the Logout button located on the top right corner of the Administration and Reporting Tool.

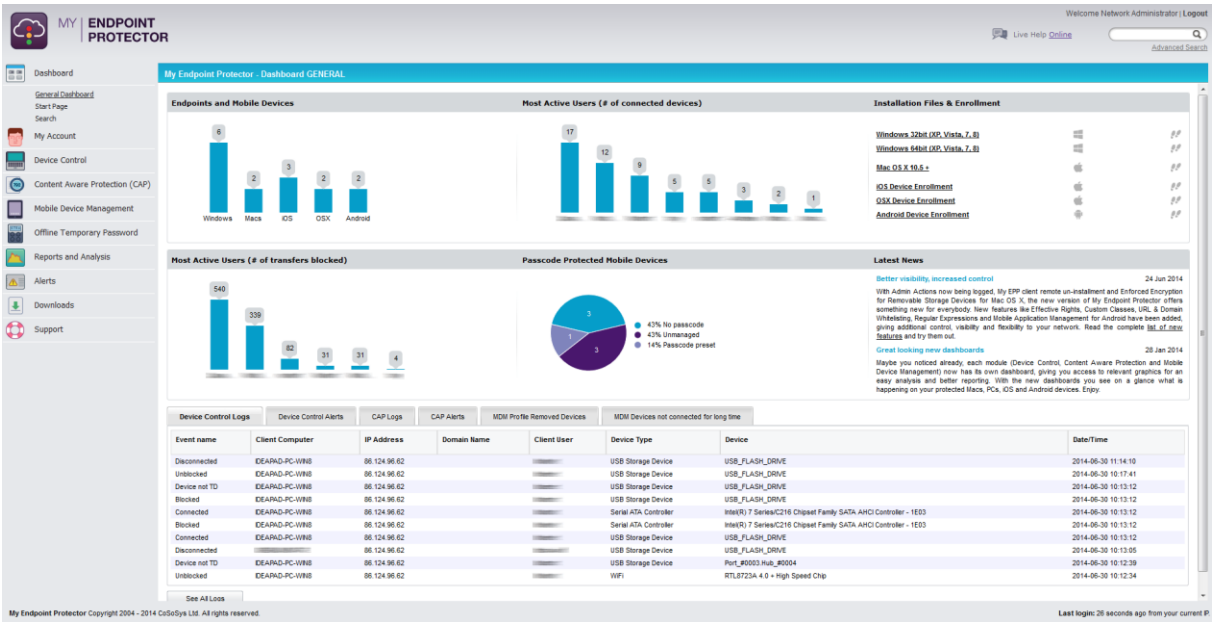
2.2. Online Administration and Reporting Tool

In the online / cloud based Administration and Reporting Tool you can manage the behavior of your protected computers and get the information regarding their device activity.

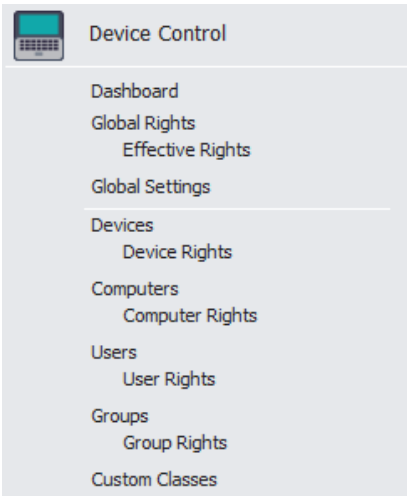
Access to Administration and Reporting Tool is restricted by a user/password pair and requires you to login.

After login into My Endpoint Protector, you will see the available modules.

Dashboard – Lets you view statistics of the server such as the number of clients and devices currently connected, the total number of protected computers, last logged action, newest added client, etc. and also provides shortcuts to the essential management tools.



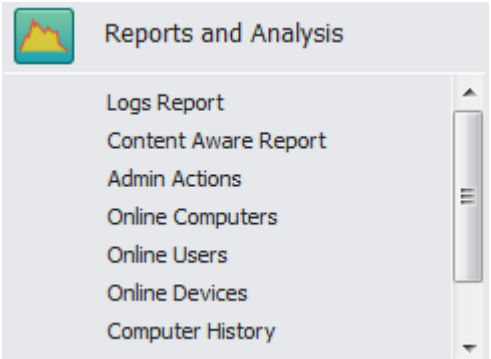
Device Control – Used for administration of Devices, Computers, Groups, and Client Users.



This is the most important module of My Endpoint Protector. In this module the administrator can set up and enforce security policies by assigning specific rights to devices, computers and computer groups.

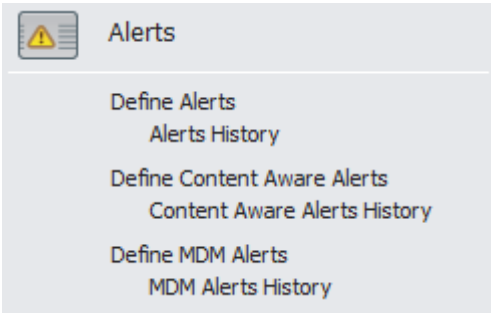
In this module, the administrator can edit, manage rights and settings or even delete devices, computers or groups. He can also create groups and add or remove client users.

Reports and Analysis – Designed to offer the administrator information regarding the past and current activity on the system (Server and Clients). It includes several sections such as Logs Report, Content Aware Report, Admin Actions, Online Computers, User History etc. Several information formats are available for view and export.



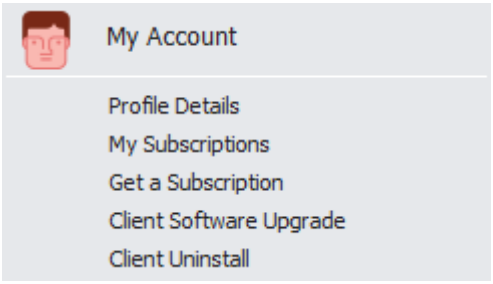
Similar to the Dashboard, this module displays usage statistics on past and current activities, but with more details.

Alerts – Allows the creation of Alerts – notifications, set up by administrators, which will alert them if a certain device was connected or accessed, a certain user performed a certain action, etc. Please see paragraph 9. “Alerts” for more details.



Offline Temporary Password – Here Offline Temporary Passwords can be defined as described in paragraph 7, "Offline Temporary Passwords".

My Account – Information related to your account can be managed here.



3. My EPP Client System Requirements

- Supported operating System:
  - Windows 8 (all versions) 32bit/64bit
  - Windows 7 (all versions) 32bit/64bit
  - Windows Vista (all versions) 32bit/64bit
  - Windows XP Home or Professional
    (Service Pack 2 is recommended)
  - Mac OS X 10.4 and 10.5+
- Administrative rights on the PC to install the MSI package
- Fully functional internet / network connection
- 1 GHz processor (or faster recommended)
- Minimum of 256 MB RAM
- 32 MB of available memory on the hard drive (plus additional space for optional offline file tracing and file shadowing)

Attention!

In case you are using an internal or external firewall, please assure that the computer you are installing the client on has the server-specified port open. By default this is port 443. In case you are behind a router, consult the device's user manual or contact the manufacturer of your device about setting up port-forwarding.

4. Client Installation

Download the correct My Endpoint Protector installer for the computer you want to protect.

Run the downloaded executable.

My Endpoint Protector Setup
MY ENDPOINT PROTECTOR
Welcome to the My Endpoint Protector Setup Wizard
The Setup Wizard will install My Endpoint Protector on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.
Sign-Up for a My Endpoint Protector account now
< Back
Next >
Cancel

It is important that you enter your correct Unique ID when requested.

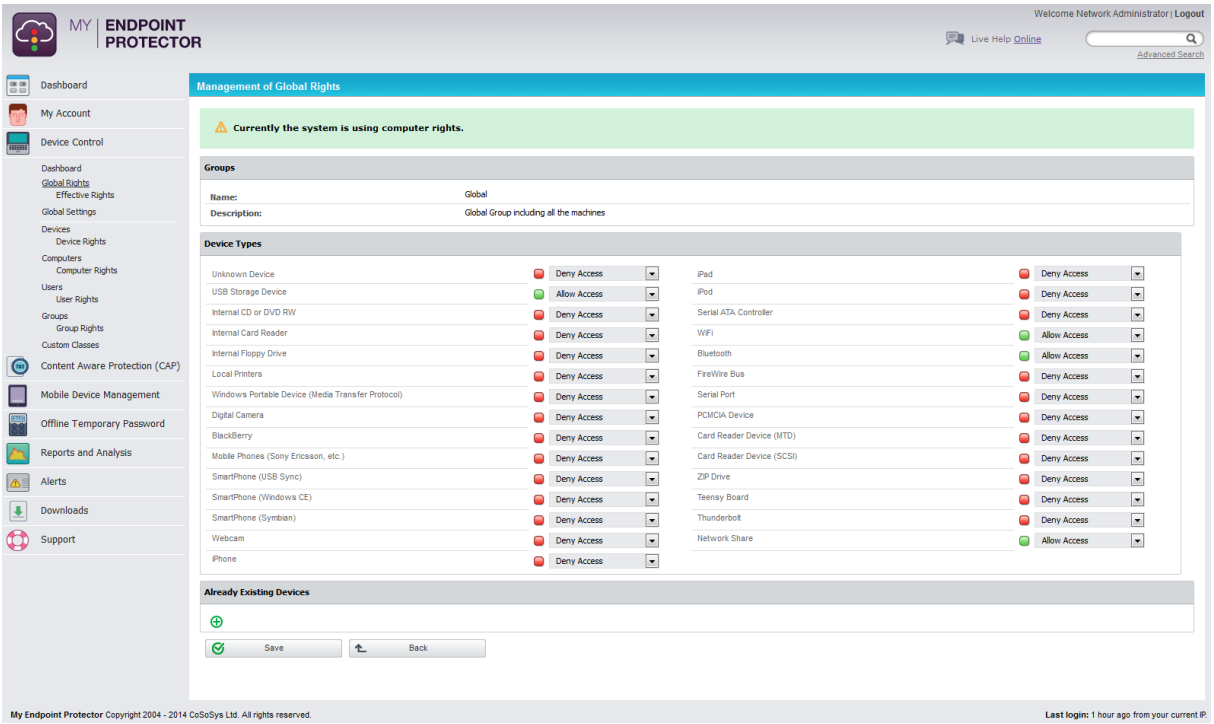
My Endpoint Protector Setup
Enter unique ID
Specify the My Endpoint Protector unique ID
Please enter your unique ID for My Endpoint Protector:
Your unique ID here
If you do not have a unique ID and a My Endpoint Protector account, please create one.
Create account
If you do not know your unique ID please login to your My Endpoint Protector account. You find the unique ID in the account info page or on the start page.
Account Login
< Back
Next >
Cancel

Please assure that your client PC has full internet access / network connectivity without any interference from firewalls, etc.

5. Device Control

5.1. Global Rights

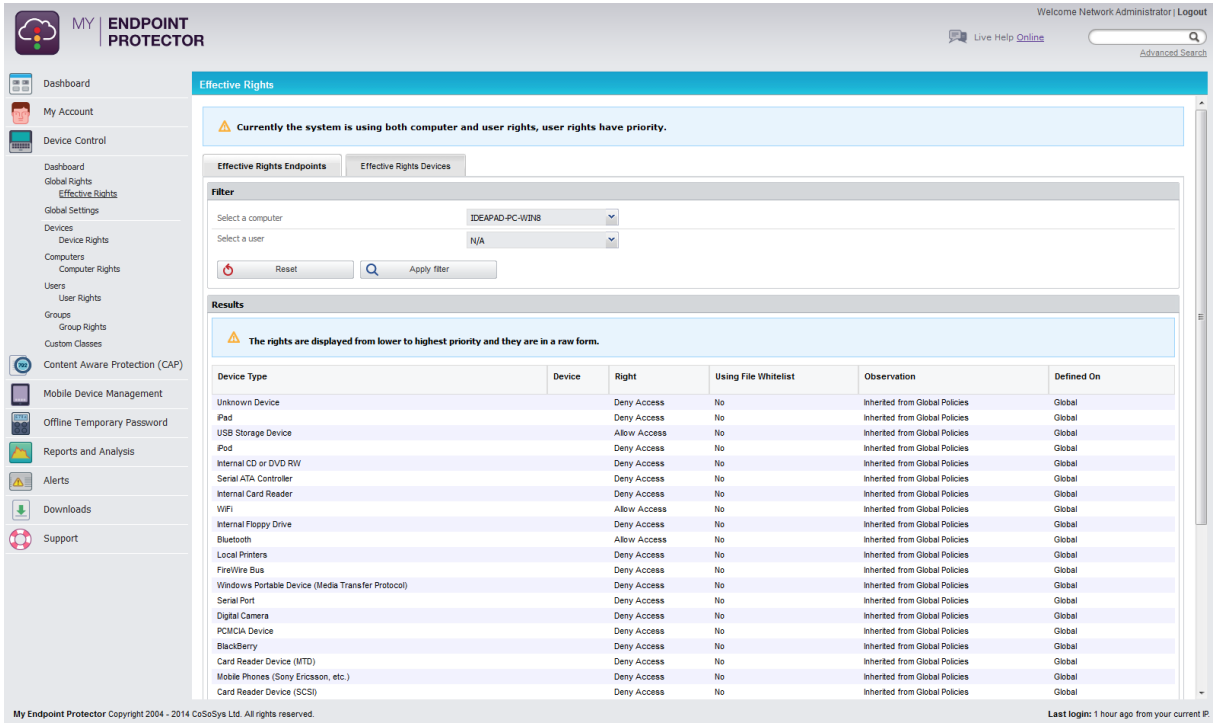
This module applies rights to computers in the entire system.



5.2. Effective Rights

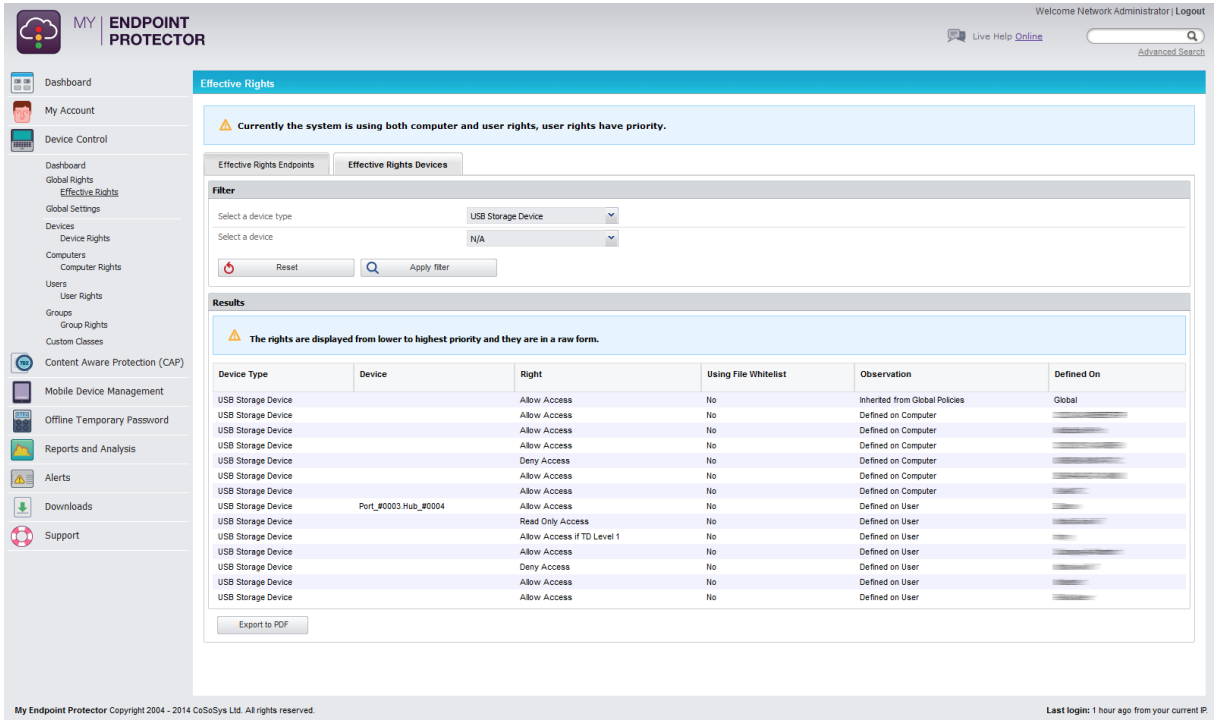
5.2.1. Effective Rights Endpoints

This module displays the rights applied for all device types at that moment in time for the entire system or a specific user/computer.


MY ENDPOINT PROTECTOR
Welcome Network Administrator | Logout
Live Help Online
Advanced Search
Dashboard
My Account
Device Control
Dashboard
Global Rights
Effective Rights
Global Settings
Devices
Device Rights
Computers
Computer Rights
Users
User Rights
Groups
Group Rights
Custom Classes
Content Aware Protection (CAP)
Mobile Device Management
Offline Temporary Password
Reports and Analysis
Alerts
Downloads
Support
Effective Rights
Currently the system is using both computer and user rights, user rights have priority.
Effective Rights Endpoints
Effective Rights Devices
Filter
Select a computer
IDEAPAD-PC-WIN8
Select a user
N/A
Reset
Apply filter
Results
The rights are displayed from lower to highest priority and they are in a raw form.
Device Type
Device
Right
Using File Whitelist
Observation
Defined On
Unknown Device Deny Access No Inherited from Global Policies Global
iPad Deny Access No Inherited from Global Policies Global
USB Storage Device Allow Access No Inherited from Global Policies Global
iPod Deny Access No Inherited from Global Policies Global
Internal CD or DVD RW Deny Access No Inherited from Global Policies Global
Serial ATA Controller Deny Access No Inherited from Global Policies Global
Internal Card Reader Deny Access No Inherited from Global Policies Global
WiFi Allow Access No Inherited from Global Policies Global
Internal Floppy Drive Deny Access No Inherited from Global Policies Global
Bluetooth Allow Access No Inherited from Global Policies Global
Local Printers Deny Access No Inherited from Global Policies Global
FireWire Bus Deny Access No Inherited from Global Policies Global
Windows Portable Device (Media Transfer Protocol) Deny Access No Inherited from Global Policies Global
Serial Port Deny Access No Inherited from Global Policies Global
Digital Camera Deny Access No Inherited from Global Policies Global
PCMCIA Device Deny Access No Inherited from Global Policies Global
BlackBerry Deny Access No Inherited from Global Policies Global
Card Reader Device (MTD) Deny Access No Inherited from Global Policies Global
Mobile Phones (Sony Ericsson, etc.) Deny Access No Inherited from Global Policies Global
Card Reader Device (SCSI) Deny Access No Inherited from Global Policies Global
My Endpoint Protector Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.
Last login: 1 hour ago from your current IP.

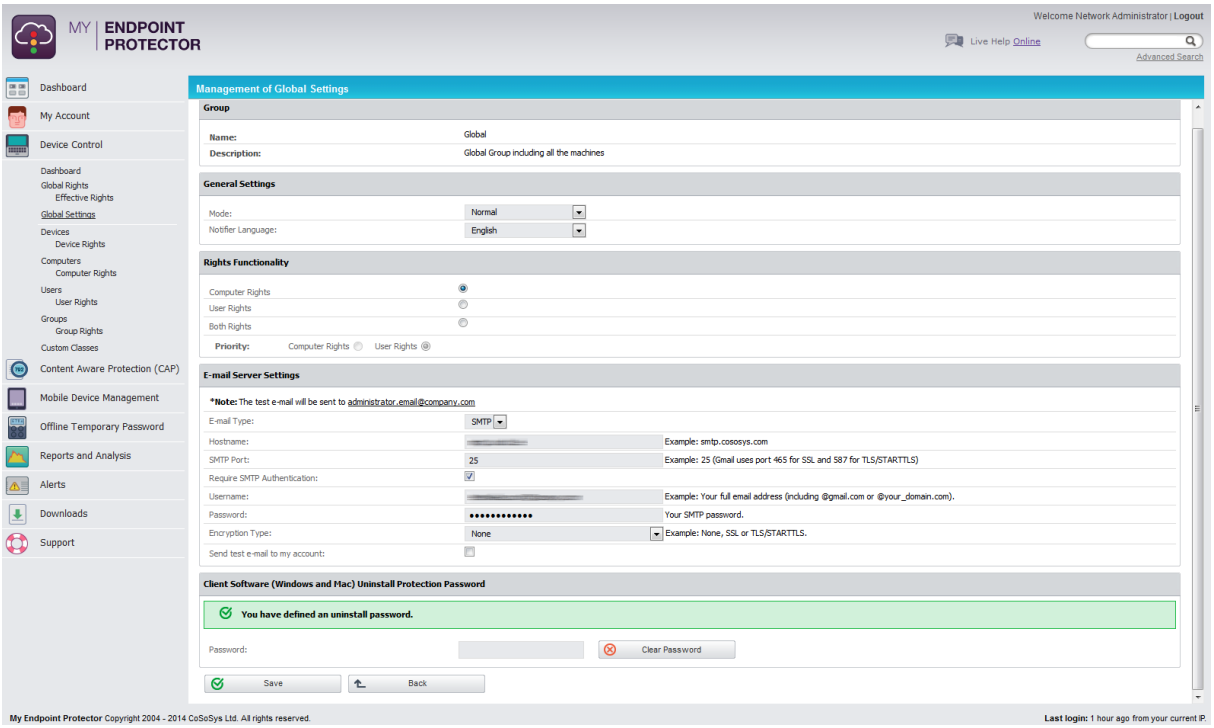
5.2.2. Effective Rights Devices

This module displays the rights applied for the selected device.


MY ENDPOINT PROTECTOR
Welcome Network Administrator | Logout
Live Help Online
Advanced Search
Dashboard
My Account
Device Control
Dashboard
Global Rights
Effective Rights
Global Settings
Devices
Device Rights
Computers
Computer Rights
Users
User Rights
Groups
Group Rights
Custom Classes
Content Aware Protection (CAP)
Mobile Device Management
Offline Temporary Password
Reports and Analysis
Alerts
Downloads
Support
Effective Rights
Currently the system is using both computer and user rights, user rights have priority.
Effective Rights Endpoints
Effective Rights Devices
Filter
Select a device type
USB Storage Device
Select a device
N/A
Reset
Apply filter
Results
The rights are displayed from lower to highest priority and they are in a raw form.
Device Type
Device
Right
Using File Whitelist
Observation
Defined On
USB Storage Device Allow Access No Inherited from Global Policies Global
USB Storage Device Allow Access No Defined on Computer
USB Storage Device Allow Access No Defined on Computer
USB Storage Device Allow Access No Defined on Computer
USB Storage Device Deny Access No Defined on Computer
USB Storage Device Allow Access No Defined on Computer
USB Storage Device Allow Access No Defined on Computer
USB Storage Device Port_#0003.Hub_#0004 Allow Access No Defined on User
USB Storage Device Read Only Access No Defined on User
USB Storage Device Allow Access if TD Level 1 No Defined on User
USB Storage Device Allow Access No Defined on User
USB Storage Device Deny Access No Defined on User
USB Storage Device Allow Access No Defined on User
USB Storage Device Allow Access No Defined on User
Export to PDF
My Endpoint Protector Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.
Last login: 1 hour ago from your current IP.

5.3. Global Settings

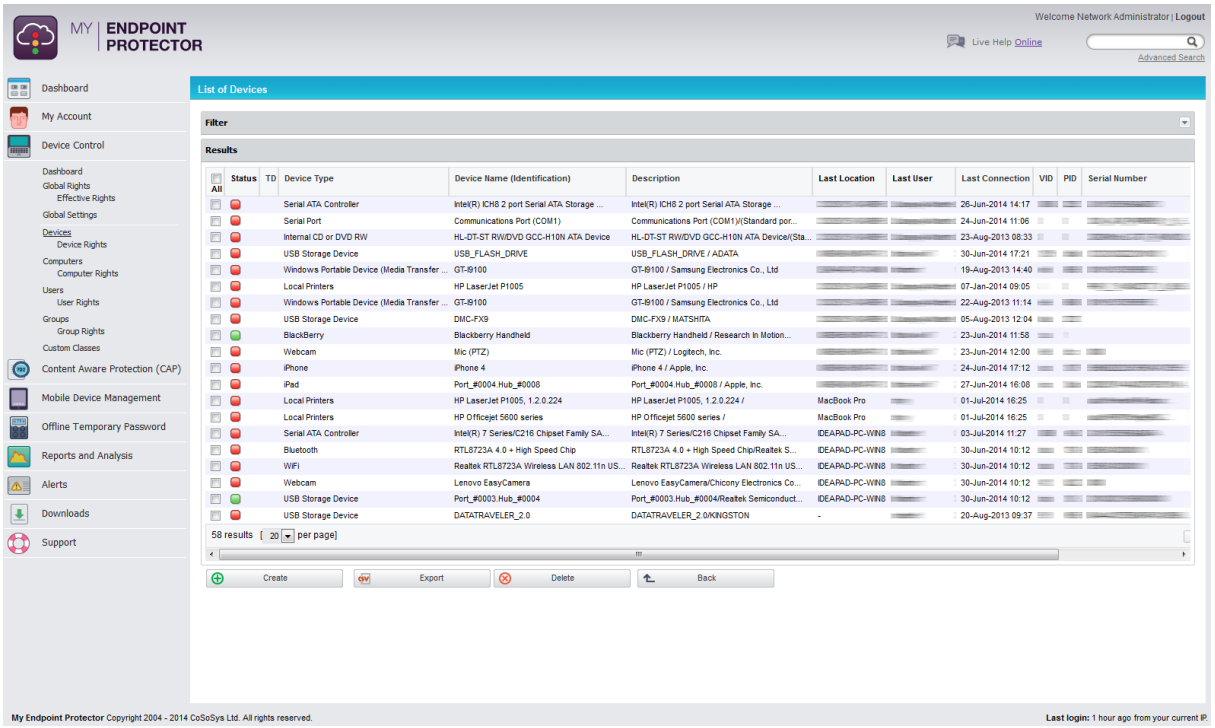
This module holds the global settings, which influence all computers within the system. If there are no settings defined for a computer, and it does not belong to a group, these are the settings it will inherit. If the computer belongs to a group, then it will inherit the settings of that group.



5.4. Devices

In this module the administrator can manage all devices in the system. My Endpoint Protector has an automatic system implemented meaning that it will automatically add any new devices connected to a protected client computers to the My Endpoint Protector database, thus making them manageable through the Administration and Reporting Tool interface.

When an unknown device is connected to one of the client computers, the device's parameters are stored in the system database as: device data (Vendor ID, Product ID, and Serial Number). The user who first used the device is stored as the default user of the device. This, however, can be changed anytime, later.



These are the actions available to the administrator in this module:

Edit, **Manage Rights, Device History, Export Device History, Delete**

Manage Rights is actually a shortcut to the Devices Rights module, and will be explained in one of the following chapters.

The status column indicates the current rights for the devices.

Red means that the device is blocked in the system.

Green means that the device is allowed on computers or users.

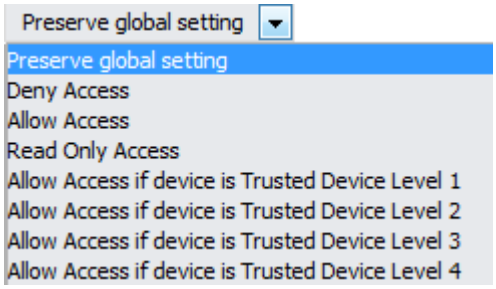
Yellow means that device is allowed on some users or computers with restrictions.

5.5. Device Rights Functionality

Endpoint Protector can handle a wide variety of devices and device types and offers several methods of usage for each device in particular. These can be found by accessing “Manage Rights” and selecting one of the relevant Rights available.

Depending on the network policy, administrators can use the following settings:

- Deny access to devices
- Allow access to devices
- Enable read-only access
- TrustedDevice Level 1 to Level 4 (applies to USB Storage Devices only)
- Block if wired network is present (applies to WiFi device control only)

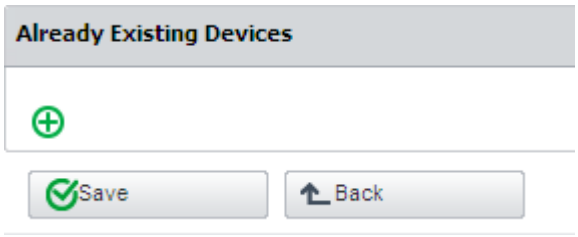

Preserve global setting
Preserve global setting
Deny Access
Allow Access
Read Only Access
Allow Access if device is Trusted Device Level 1
Allow Access if device is Trusted Device Level 2
Allow Access if device is Trusted Device Level 3
Allow Access if device is Trusted Device Level 4

5.5.1. Give / Deny Access to Devices

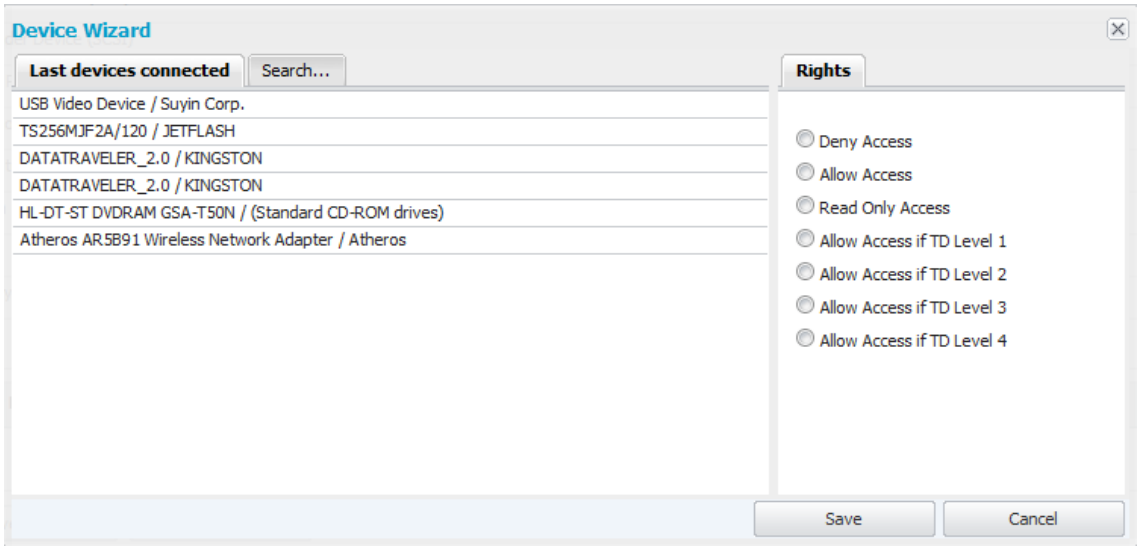
With this option the administrator can give or deny complete access to a certain device making it usable or obsolete for a certain group or computer.

The administrator can configure these settings for each device individually and can also choose for what computer(s) and group(s) they will apply to.

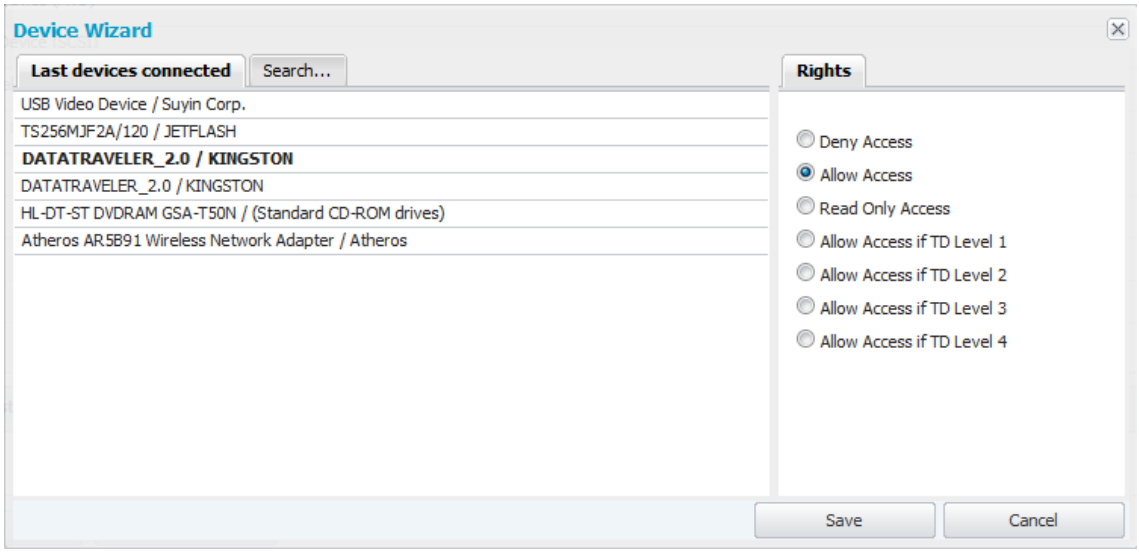
Select the device, computer or group you wish to manage rights for and click the + (plus) button at the bottom of the page, under “Already Existing Devices”.



Once you do that, the Device Wizard will appear, allowing you to select the device(s) you wish to manage.



Selecting a device will allow you to select one of the rights for that device.



Click "Save" to store your changes.

The device(s) you selected will appear in the "Already Existing Devices" section.

To add more devices, simply repeat the steps mentioned above.

To change or delete added devices use either "Rights Wizard" or "Remove" action buttons.

5.5.2. Enable Device Read-Only Access

With this option the administrator can enable read-only access to devices preventing the deletion or alteration of data on the device(s).

The administrator can configure each device individually and can also choose for what computer and group it will apply to.

5.5.3. TrustedDevice Level 1 to Level 4

This option has four levels. Selecting either one of these implies that you already have knowledge and understanding of how TrustedDevices™ and EasyLock™ work.

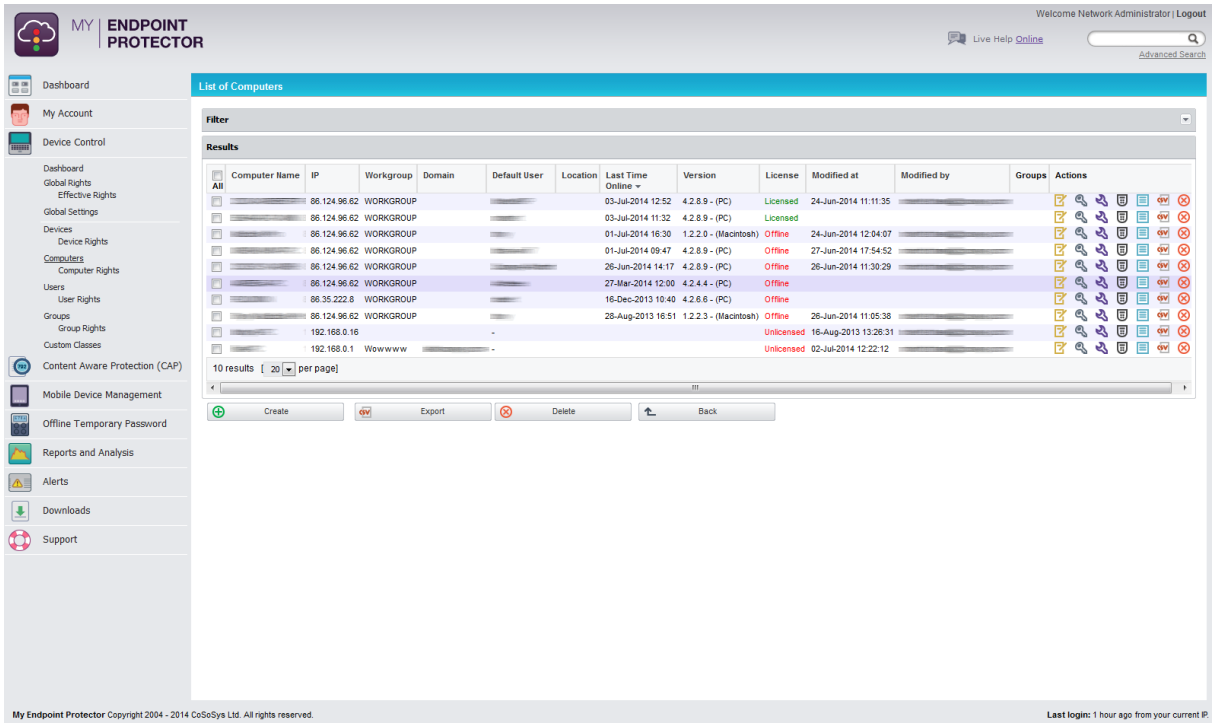
For more information, please see section “How a Level 1 TrustedDevice Works” in this user manual.

5.5.4. WiFi - Block if wired network is present

With this option the administrator can disable the WiFi connection, while a wired network connection is present. The WiFi connection will be available when the wired network is not present.

5.6. Computers

This is the module responsible for managing the client computers.



The available actions here are:

Edit, **Manage Rights**, **Manage Settings, Offline Temporary Password, Computer History, Export Computer History** and **Delete**. The Manage Rights and Manage Settings are links to their respective modules, which will be explained in their own chapter.

For a better organization and manageability, a computer can be assigned as belonging to a Group (several computers within the same office, a group of computers, which will have same access rights or settings).

5.6.1. Computer Self Registration

The client computers have a registration mechanism. This self-registration mechanism is running once after the My Endpoint Protector Client software is installed on a client computer.

During the installation of the My Endpoint Protector Client, you will be asked to enter your **unique ID** for client installation.

This will bind the client software to your My Endpoint Protector account and the client will then communicate to the server its existence in the system.

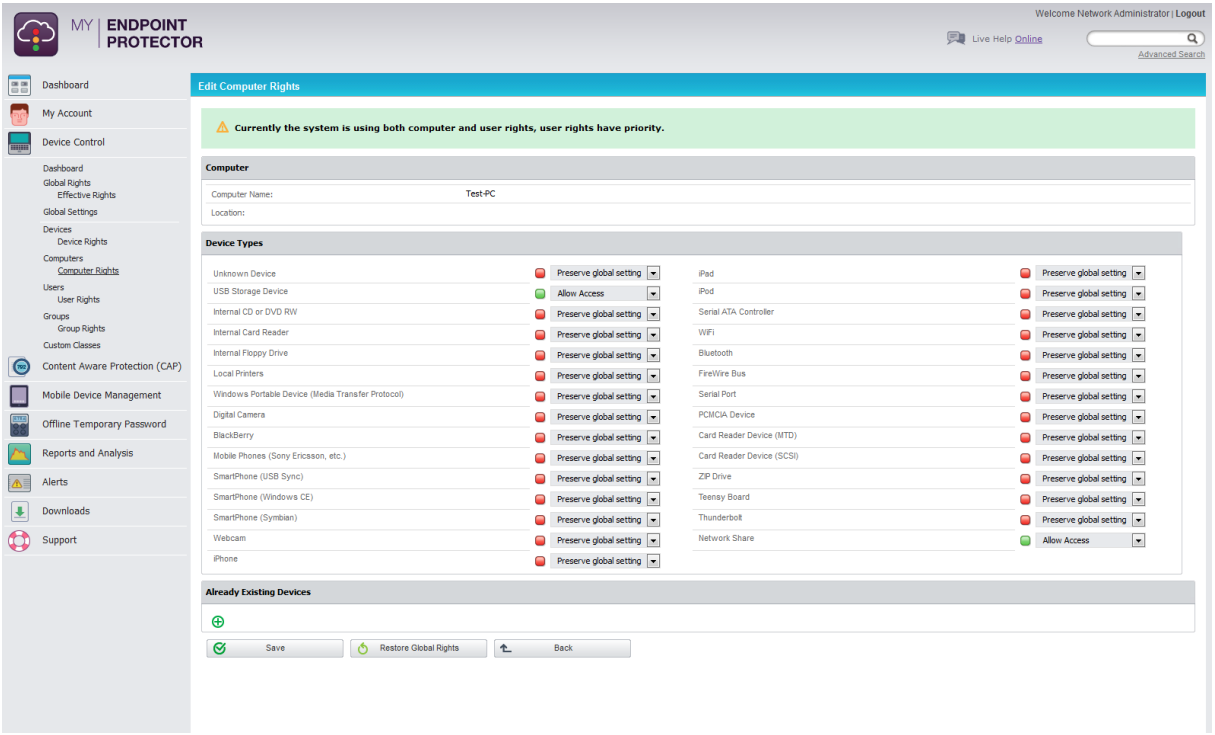
The server will store the information regarding the client computer in the system database and it will assign a license to the client computer.

Note!

The self-registration mechanism acts whenever a change in the computer licensing module is made, and also each time the application client is reinstalled. The owner of the computer is not saved in the process of the self-registration.

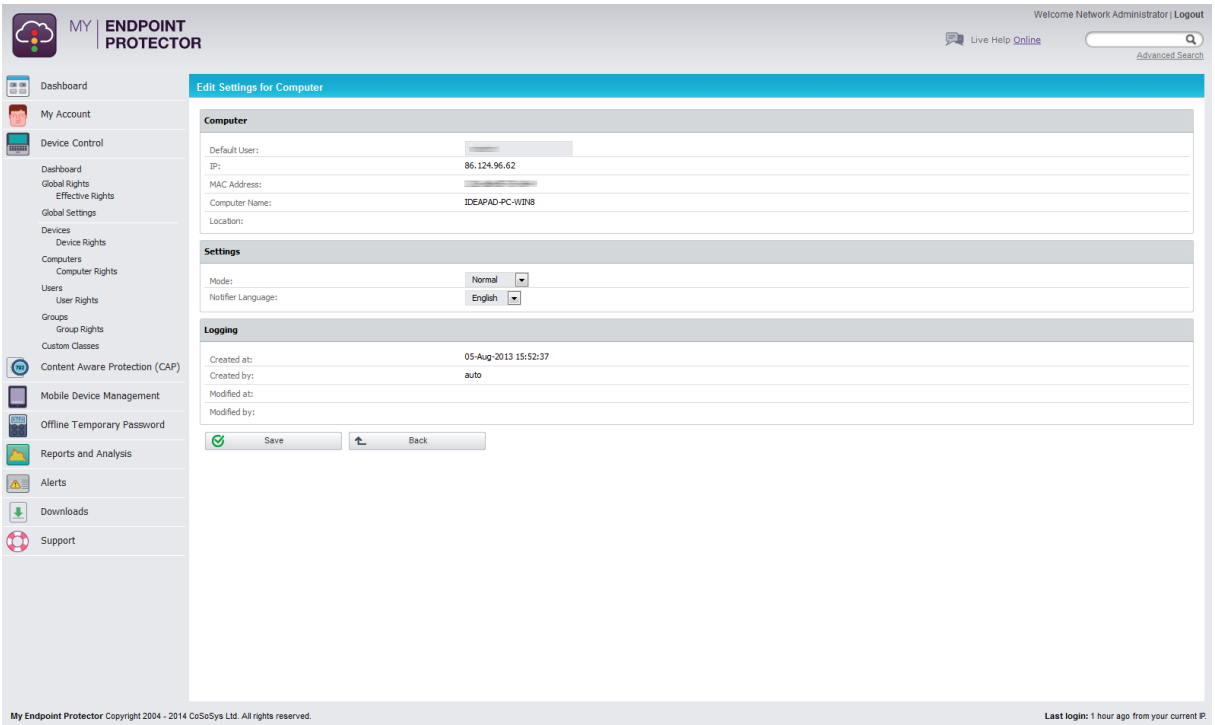
5.7. Computer Rights

This module will allow administrators to specify what device types and also what specific device(s) can be accessible from a single or all computers.



5.8. Computer Settings

This module will allow the administrator to edit the settings for each computer. It is accessible from the Computers tab, where you have to click on the "Settings" ( ) button.

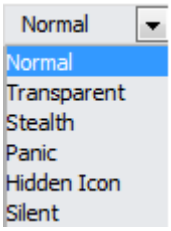


Defining custom settings for all computers is not necessary, since a computer is perfectly capable of functioning correctly without any manual settings defined. It

will do this by either inheriting the settings of a group to which it belongs or, if not possible, the global settings, which are mandatory and exist in the system with default values.

5.9. Modes for Computers and Groups

My Endpoint Protector features several functionality modes for computers and groups. These modes can be set through “Computer Settings”, ”Group Settings” or “Global Settings” (applied by default).You can change these at any given time.



There are six modes from which you can choose:

- Normal Mode (default mode of Endpoint Protector)
- Transparent Mode
- Stealth Mode
- Panic Mode
- Hidden Icon Mode
- Silent Mode

5.9.1. Transparent Mode

This mode is used if you want to block all devices, but you don’t want the user to see and know anything about My Endpoint Protector activity.

- no system tray icon is displayed
- no system tray notifications are shown
- everything is blocked, regardless if authorized or not
- Administrator receives alerts (dashboard also shows alerts) for all activities

5.9.2. Stealth Mode

Similar to Transparent mode, Stealth mode allows the administrator to monitor all users and computers activities and actions with all devices allowed.

- No system tray icon is displayed
- no system tray notifications are shown
- everything is allowed (nothing is blocked regardless of what activity)
- Administrator receives alerts (dashboard shows also alerts) for all activities

5.9.3. Panic Mode

If Stealth Mode and Transparent Mode are set manually, Panic Mode will be set automatically by the system, when it considers it necessary.

- system tray icon is displayed
- notifications are displayed
- everything is blocked regardless if authorized or not
- Administrator receives alert (dashboard also shows alerts) when PCs are going in and out of Panic mode

5.9.4. Hidden Icon Mode

The Hidden Icon Mode is similar to the Normal mode, the difference consisting in the fact that the Agent is not visible to the user.

- no system tray icon is displayed
- no system tray notifications are shown
- all set rights and settings are applied

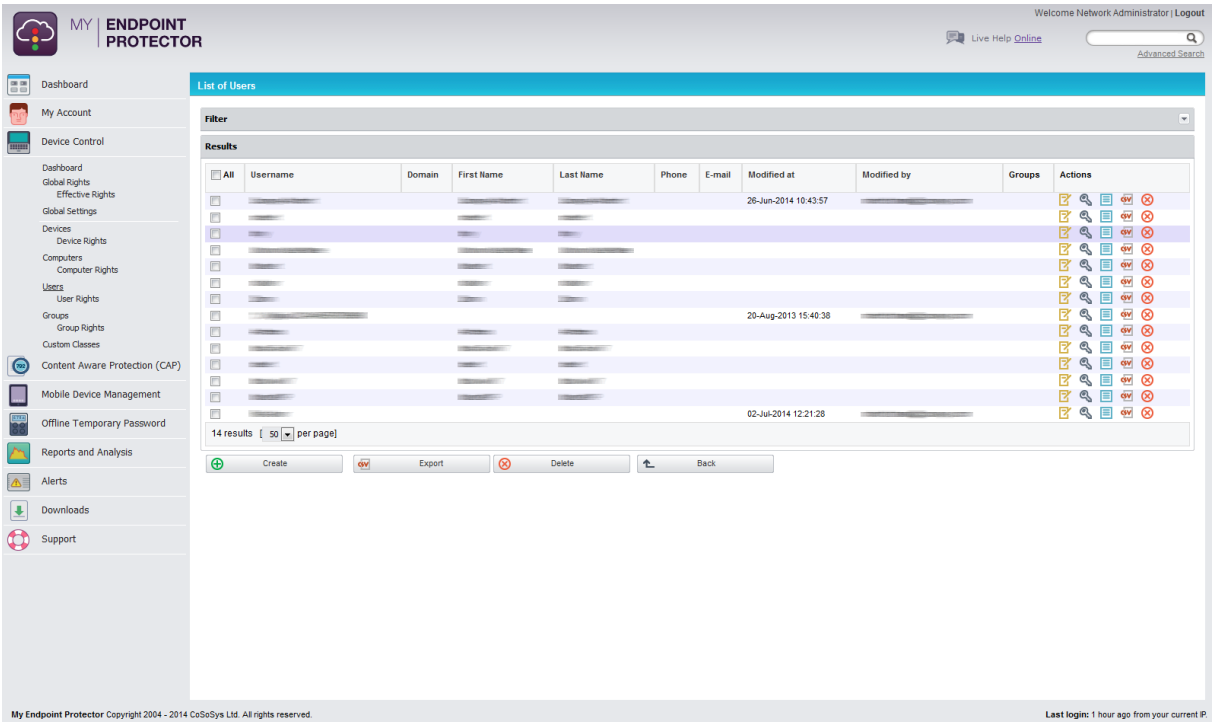
5.9.5. Silent Mode

The Silent Mode is similar to the Normal mode, the difference consisting in the fact that the notifications do not pop-up to the user.

- system tray icon is displayed
- no system tray notifications are shown
- all set rights and settings are applied

5.10. Users

The client users are the end users who are logged on a computer on which the My Endpoint Protector Client software is installed.



This module has a self-completing mechanism: as soon as a user has some activity on the system and he is new in the system, he will be added to the system database.

These are the actions available to the administrator in this module:

Edit, Manage Rights, User History, Export User History and **Delete**.

There are two users created by default during the installation process of My Endpoint Protector.

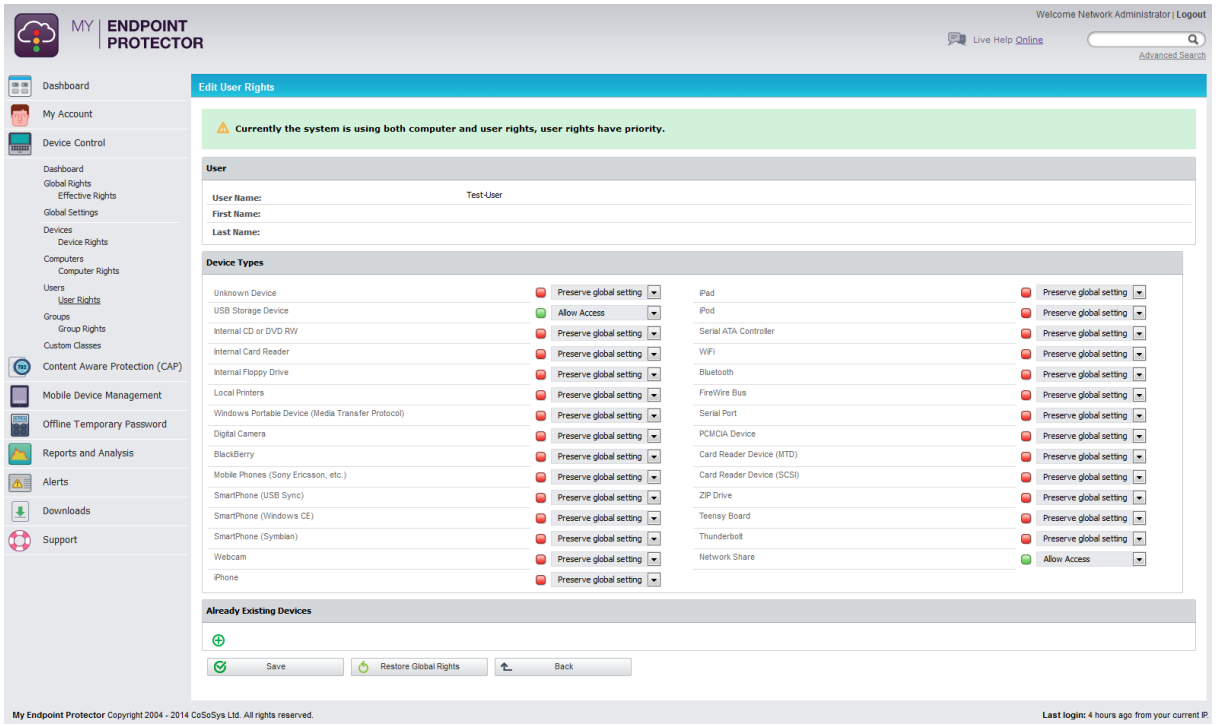
noUser – is the user linked to all events performed while no user was logged into the computer. Remote users' names who log into the computer will not be logged and their events will be stored as events of noUser. Another occurrence of noUser events would be to have an automated script/software, which accesses a device when no user is logged into the specific computer.

autorunUser – indicates that an installer has been launched by Windows from the specific device. It is the user attached to all the events generated by the programs launched from that specific device when Autoplay is enabled in the Operating System.

The users can be arranged in groups for easier management at a later point.

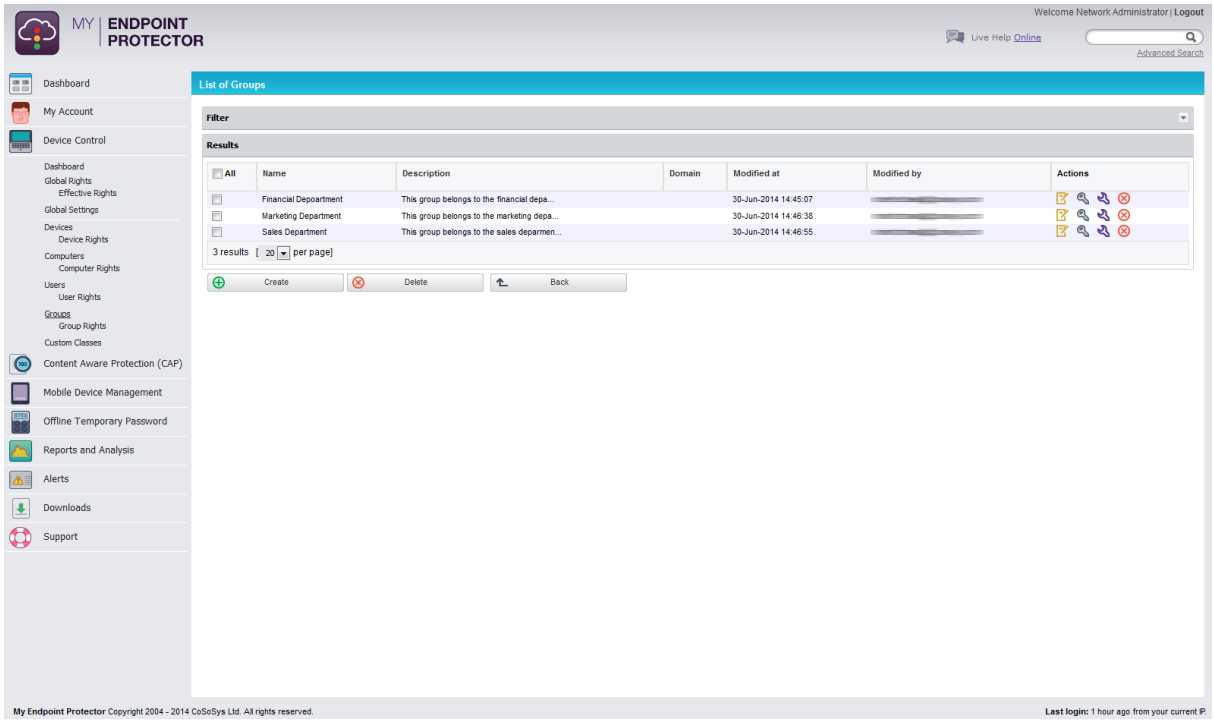
5.11. User Rights

This module is built around the user, allowing administrators to manage rights of access to devices per users.



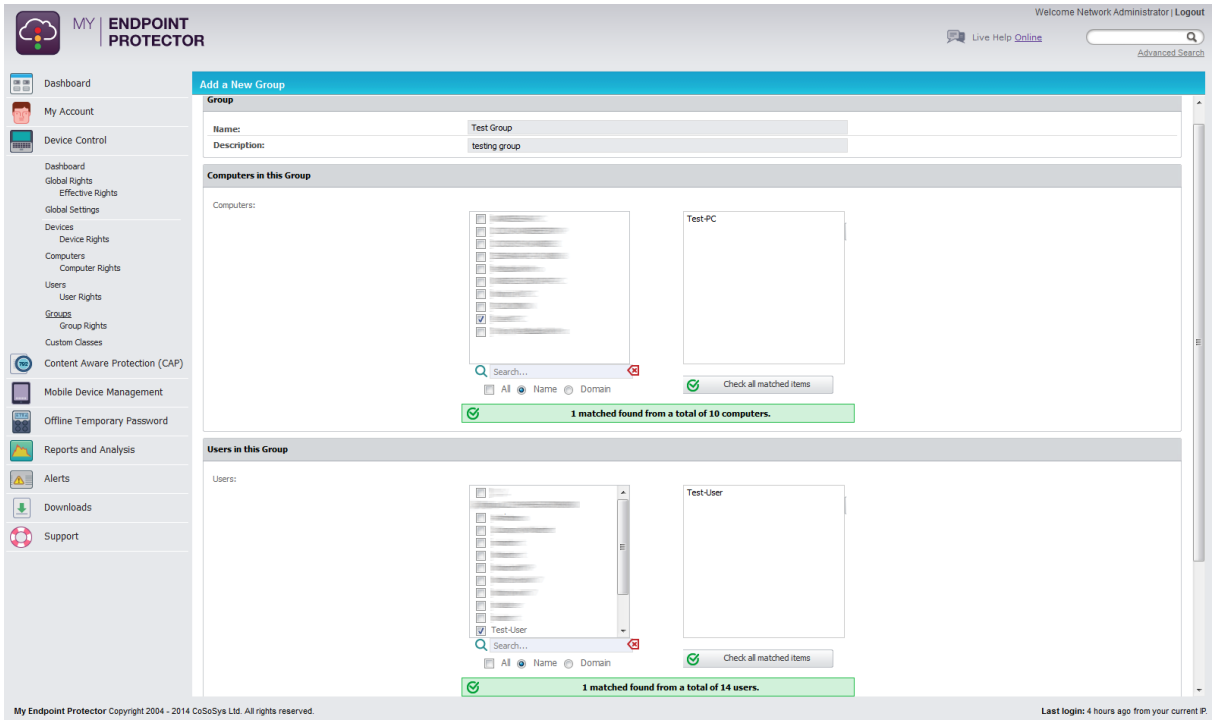
5.12. Groups

This module is responsible for editing groups. **Edit**, **Manage Rights**, **Manage Settings** and **Delete** are the commands available from this section.



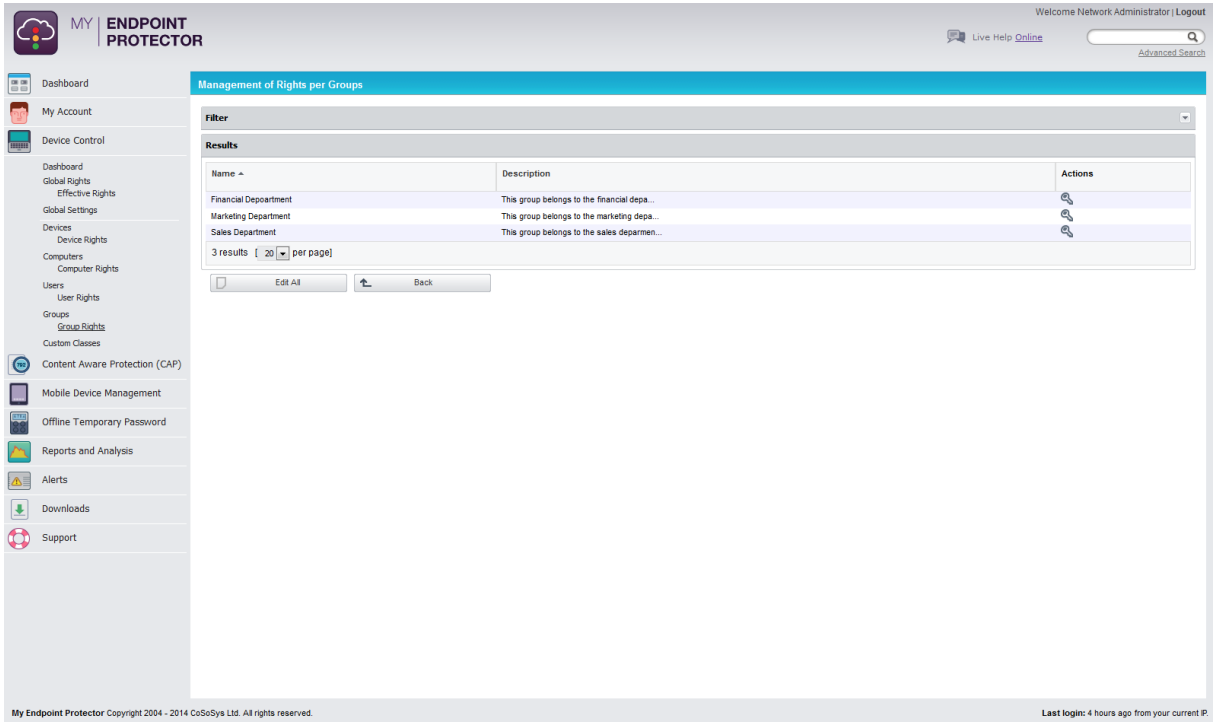
Grouping computers and client users will help the administrator to manage the rights or settings for these entities in an efficient way. This can be done from the Group Rights and Group Settings tabs.

When creating a new group there is the possibility to add multiple users / computers simultaneously, by using the checkboxes and the option “Check all matched items”.



5.13. Group Rights

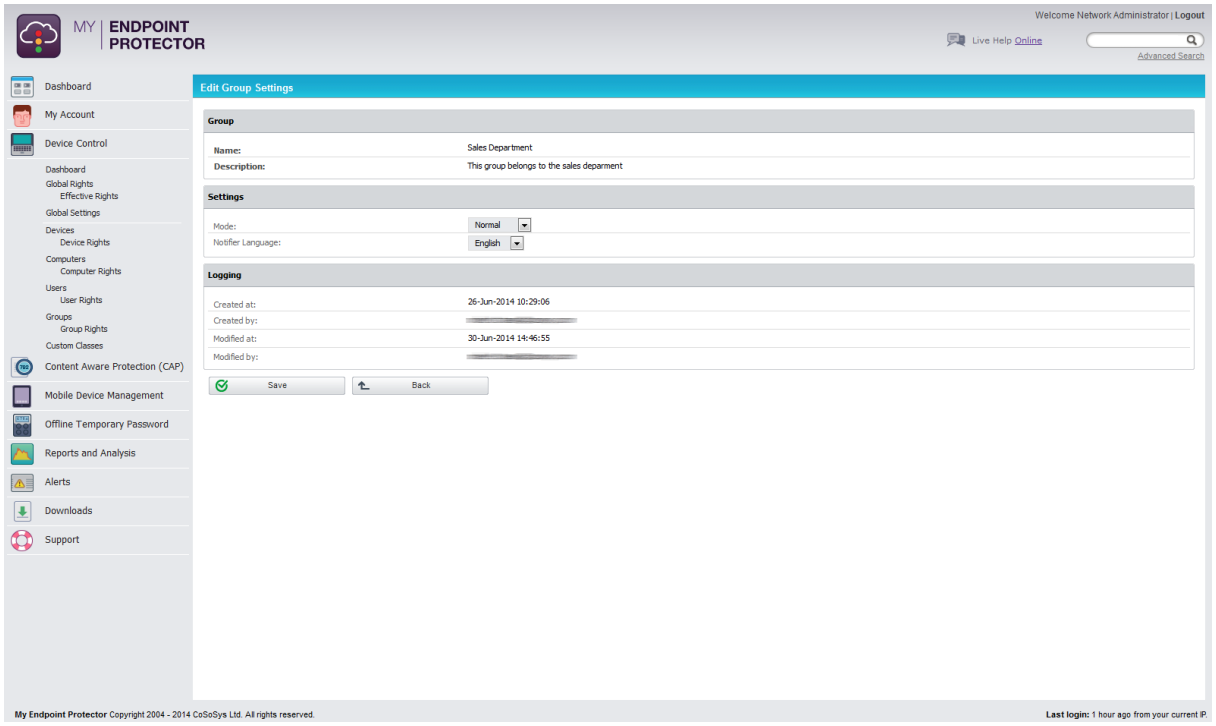
This module is built around a group of computers and/or users, allowing administrators to manage rights of access to devices per groups.



The administrator can use the "Edit All" action here to edit rights for all groups at once.

5.14. Group Settings

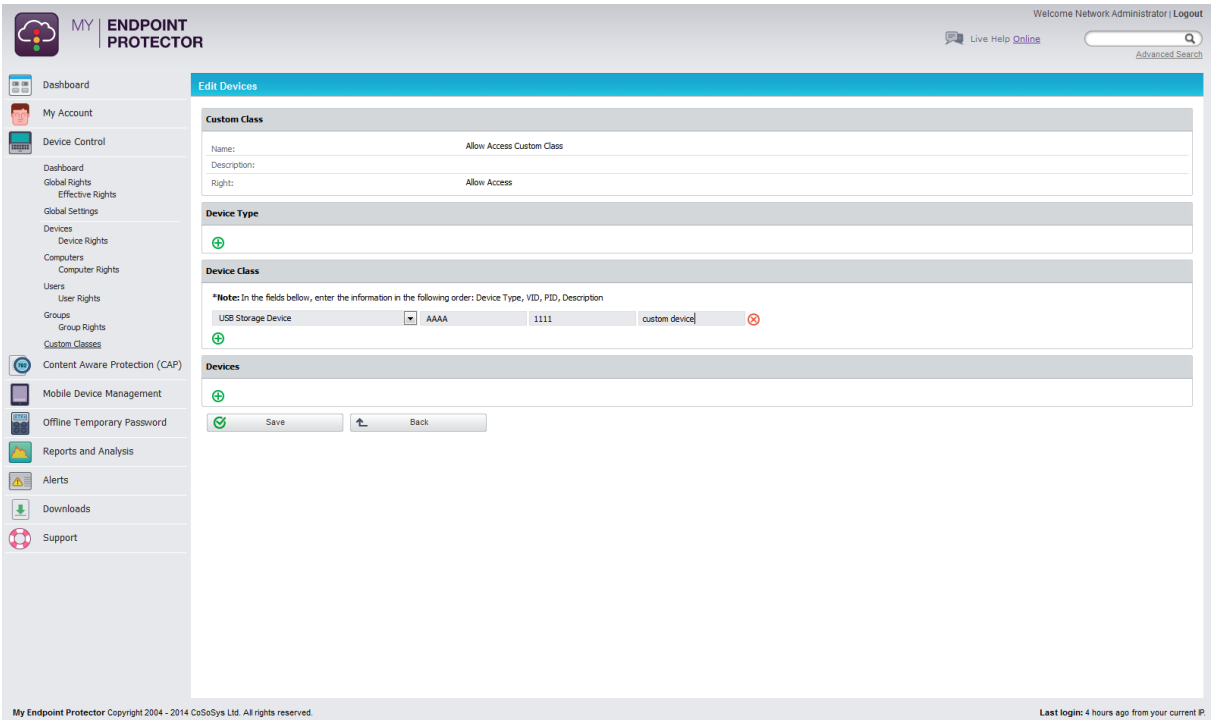
This module will allow the administrator to edit group settings. It is accessible from the Groups tab, where you have to click on the "Settings" ( ) button.



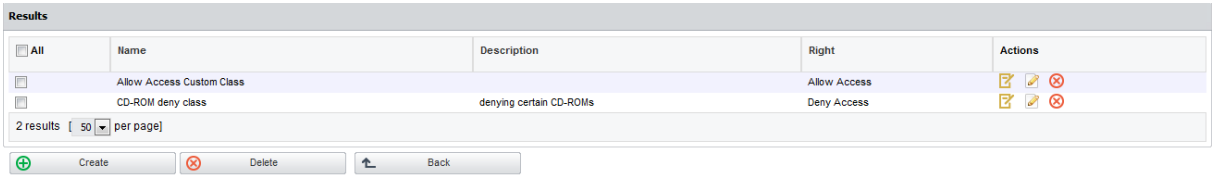
Creating groups of Computers makes editing of settings easier and more convenient.

5.15. Custom Classes

This module is responsible for creating new classes of devices for an easier management inside the system. It is a powerful function especially for devices belonging to the same vendor and/or being the same product (same VID and/or PID).



By selecting Device Control > Custom Classes, the administrator is able to create and edit custom classes by adding new entities to the existing ones.



When creating a new custom class or editing an existing one, the administrator may provide a unique name and a short description, followed by the specification of the rights that will be automatically applied to all included devices.

Note!

The rights set for a Custom Class will override all the other existing rights for the devices included in the newly created class and they will apply for any Endpoint Protector Client PC.

Example:

For the case above, we created an *Allow Access Custom Class* and set "Allow access" rights to devices of type *USB Storage*. Let's say that USB Storage Devices have "Deny access" right set on Client PC CIP0. Once the custom class

Allow Access Custom Class is created all USB Storage devices will have access, even if on the Client PC CIP0 they have “Deny access”.

6. Content Aware Protection

This module allows the administrator to setup and enforce strong content filtering policies for selected users, computers or groups and take control over the risks posed by accidental or intentional file transfers of sensitive company data, such as:

- Personally Identifiable Information (PII): social security numbers (SSN), driving license numbers, E-MAIL addresses, passport numbers, phone numbers etc.
- Financial and credit card information: credit card numbers for Visa, MasterCard, American Express, JCB, Discover Card, Diners Club, bank account numbers etc.
- Confidential files: sales and marketing reports, technical documents, accounting documents, customer databases etc.

To prevent sensitive data leakage, My Endpoint Protector closely monitors all activity at endpoints and other exit ways:

- Transfers on portable storage and other media devices (USB Drives, external hard-disks, CDs, DVDs, SD cards etc.), either directly or through encryption software (e.g. EasyLock)
- Transfers on local networks
- Transfers via Internet (E-MAIL clients, file sharing application, Web Browsers, Instant Messaging, Social Media)
- Transfers to the cloud (iCloud, Google Drive, Dropbox, Microsoft SkyDrive)
- Transfers through Copy & Paste / Cut & Paste
- Print screens

Note!

The Content Aware Protection feature requires separate licensing, in addition to the My Endpoint Protector license for Device Control.

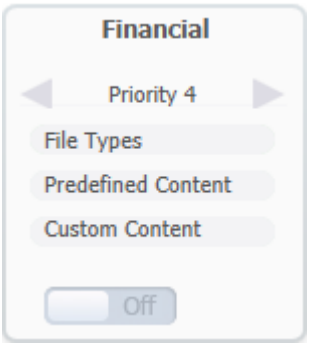
6.1. Content Aware Policies

Content Aware Policies are sets of rules for sensitive content detection and blocking, enforced on selected network entities (users, computers, groups, departments).

A content aware policy is made up of four elements:

- Policy Type: defines for which type of OS the policy applies, Windows or Macintosh
- Policy Action: defines the type of action to be performed: reporting of sensitive content detection or blocking and reporting of sensitive content transfers
- Policy Filter: specifies the content to be detected, including: file type filtering, predefined content filtering and custom content filtering
- Policy Control Points: establishes the transfer destinations to be monitored

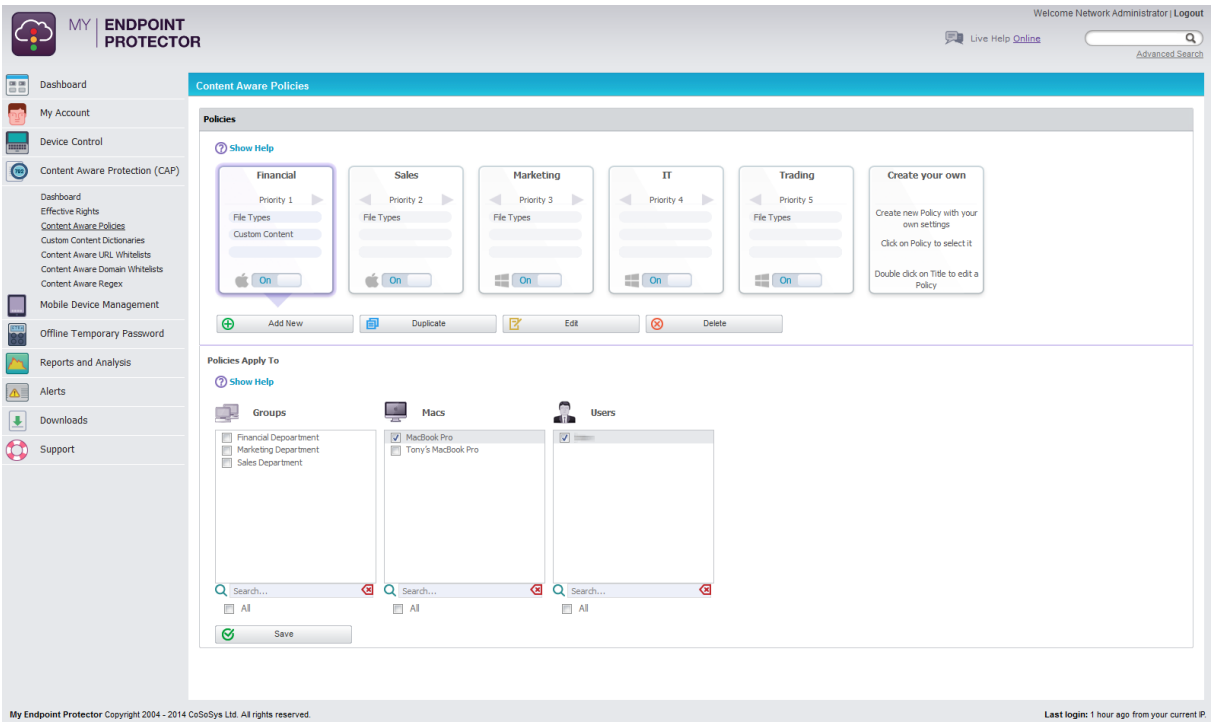
For example, a policy can be setup for the Financial Department of the company to block Excel reports sent via E-MAIL or to report all transfers of files containing personally identifiable and financial information (e.g. credit card numbers, E-MAILS, phone numbers, social security numbers etc.).



Additionally, each company can define its own sensitive content data lists as Custom Content Dictionaries corresponding to their specific domain of activity, targeted industry and roles. To ease this task, the Content Aware Protection module comes with a predefined Custom Content Dictionary that covers the most used sets of confidential terms and expressions.

Exactly like for Device Control policies, the Content Aware policies continue to be enforced on a computer even after it is disconnected from the company network.

The administrator can easily create and manage Content Aware Policies application inside the network from the Content Aware Protection -> Content Aware Policies submenu option.



The available actions are: **Add New**, **Duplicate**, **Edit** and **Delete**. A new policy can be created also by clicking on the "Create your own" policy icon. An existing policy can be edited also by double-clicking the upper part of the policy icon.

By selecting a policy, the groups, computers and users on which the selected policy applies, will be highlighted for an easier policy management. The administrator can then uncheck previously enabled entities for monitoring or check new ones. All changes performed on the page are applied after clicking "Save".

6.1.1. Priorities for Content Aware Policies

One or more Content Aware Policy can be enforced on the same computer, user or group. To avoid any conflicts between the applied rules, a prioritization of policies is performed through a left-to-right ordering. The leftmost policy has the highest priority (Priority 1), while the rightmost policy has the lowest priority. Changing priorities for one or more policies can be performed by moving the policy to the right or to the left with a simple click on the left arrow for higher priority or on the right arrow for lower priority.

6.1.2. How Content Aware Policies Work

Content Aware Protection is a very versatile tool, where granular implementation of the desired actions regarding report and/or block and report of files can be performed.

A Content Aware Policy is a set of rules for reporting or blocking & reporting the selected information. All the other options left unchecked will be considered as Ignored by My Endpoint Protector.

When applying two policies to the same PC, it is possible to block one type of file, for example PNG files, when they are uploaded through Mozilla Firefox, while with a second policy to report only PNG files when they are uploaded through Internet Explorer. In the same way it is possible to report only files that contain confidential words from a selected dictionary and are sent through Skype, while with the second policy to block the same files if they are sent through Yahoo Messenger and NateOn Messenger. Similar to this example: it is possible to create combinations that will allow you to block a file type or a file that contains predefined content/custom content/regular expression for one application, while letting it through and report it only for another application.

The following rules are used in the application of one or more Content Aware Policies on a computer/user/group/department for each separately selected item (e.g. a specific file type, predefined information or a custom content dictionary):

Policy A with Priority 1	Policy B with Priority 2	Policy C with Priority 3	Endpoint Protector Action
IGNORED	IGNORED	IGNORED	Information will not be blocked or reported.
IGNORED	IGNORED	*REPORTED*	Information will be reported.
IGNORED	*REPORTED*	*REPORTED*	Information will be reported.
REPORTED	*REPORTED*	*REPORTED*	Information will be reported.
IGNORED	IGNORED	**BLOCKED**	Information will be blocked.
IGNORED	**BLOCKED**	**BLOCKED**	Information will be blocked.
BLOCKED	**BLOCKED**	**BLOCKED**	Information will be blocked.
IGNORED	*REPORTED*	**BLOCKED**	Information will be reported.
IGNORED	**BLOCKED**	*REPORTED*	Information will be

			blocked.
REPORTED	IGNORED	**BLOCKED**	Information will be reported.
BLOCKED	IGNORED	*REPORTED*	Information will be blocked.
REPORTED	**BLOCKED**	IGNORED	Information will be reported.
BLOCKED	*REPORTED*	IGNORED	Information will be blocked.

Attention!

The information left unchecked when creating a policy will be considered as Ignored by My Endpoint Protector and **NOT AS ALLOWED**.

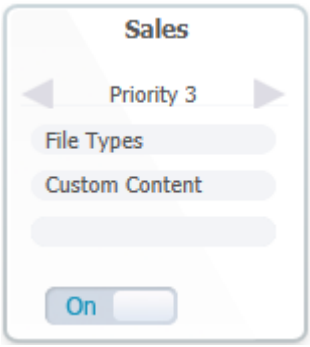
6.1.3. Types of Content Aware Policies

Depending on the selected content to detect, a policy can be classified in:

- **File Type Filter Policy**: detects/blocks all transfers of preselected file types, including preselected file types archived in zip files with no password protection
- **Predefined Content Policy**: detects/blocks all file transfers containing Credit Card and/or Personal Identifiable information
- **Custom Content Policy**: detects/blocks all file transfers containing terms from a preselected Custom Content Dictionary

Combined policies can be created by selecting several filter types for the same policy.

An example of a combined Content Aware Policy for the Sales Department to detect specific file types and custom terms is shown below.



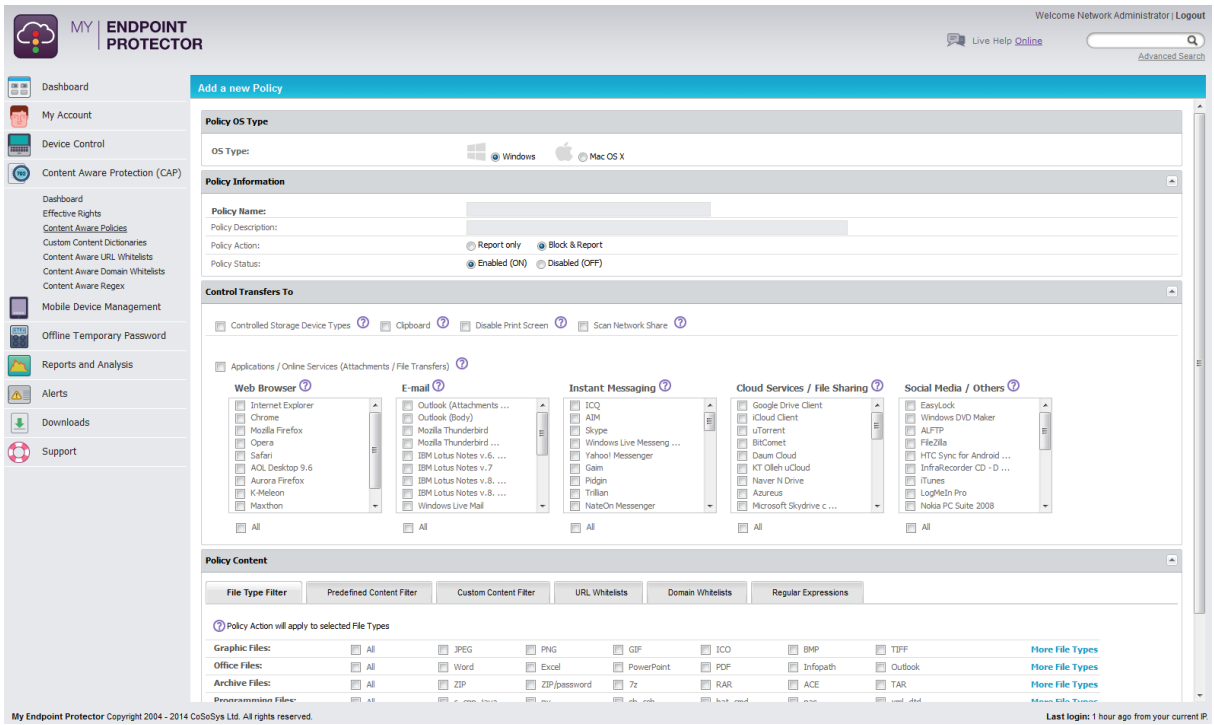
Depending on the selected content to monitor, the icon corresponding to the newly created policy will highlight the specific selected filters.

Note!

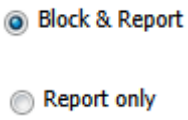
Content Aware Policies apply also to File Whitelist. This means that all files that were previously whitelisted will be inspected for sensitive content detection, reported and / or blocked according to the defined policy.

6.1.4. Setting up Content Aware Policies

To set up a Content Aware Policy, go to Content Aware Protection -> Content Aware Policies and click on the Create Your Own Policy icon or push the "Add Policy" button. This will open the Add a new Policy window, which will allow setting the parameters of the newly created policy.



A policy can be enforced to detect & report all transfers of sensitive content data and/or block all transfers:



Attention!

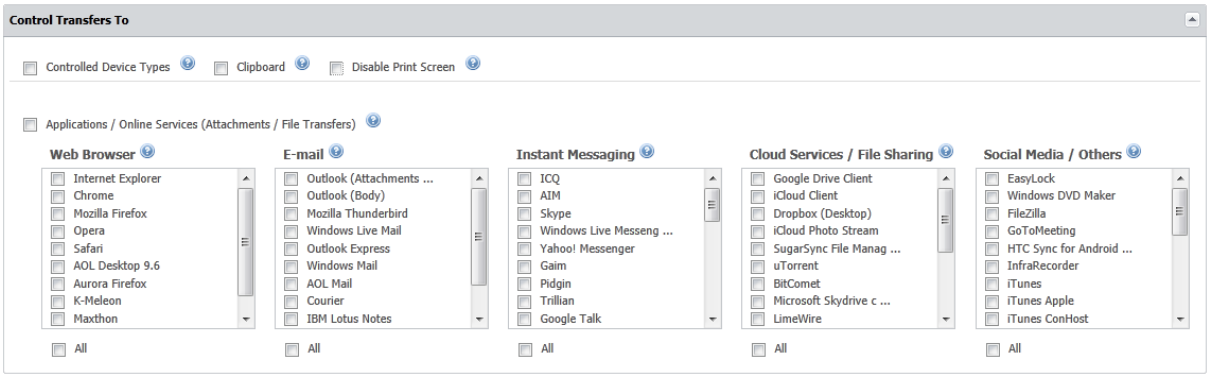
The Block & Report action will block all file transfers on the selected network entity. We recommend using the Report only action initially to detect but not block data transfers. This way, no activity will be interrupted and you can gain a better view of data use across your network.

By default, data control is turned off. To activate the defined content rules, a newly created policy must be enabled (ON). The policy status can be changed later by using the simple ON/OFF switch from the policy icon:

Note!

An enabled (ON) Policy will be enforced only after selecting the network entities to be monitored.

To complete the policy definition, the transfer destinations to be monitored must be selected and the content to be detected must be specified.



There are five main categories of transfer destinations to control:

- Controlled device types: comprises the list of all removable devices registered to My Endpoint Protector.

Note!

For Controlled Device Types category, My Endpoint Protector will monitor file transfers both to and from removable media.

- Clipboard: refers to all content captured through Copy & Paste and Cut & Paste operations
- Disable Print Screen: refers to the screen capture option
- Scan Network Share: refers to content uploaded to local networks
- Applications / Online Services (Attachments / File Transfers): comprises Web Browsers, E-MAIL Clients, IM, File Sharing, Social Media/Others.

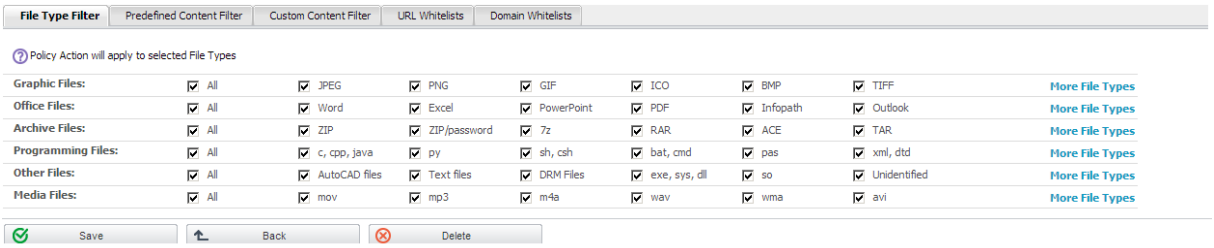
Type	List of Applications
Web Browsers	Internet Explorer, Mozilla Firefox, Chrome, Opera, Safari, SeaMonkey, Maxthon, AOL Destop 9.6, K-Meleon, Aurora Firefox
E-MAIL Clients	Microsoft Office Outlook, Mozilla Thunderbird, Windows Live Mail, Outlook Express, Windows Mail, AOL Mail, Opera Mail, SeaMonkey Mail, Courier, IBM Lotus Notes, GroupWise Client
Instant Messaging	AIM, eBuddy, MySpace IM, ICQ, Google Talk, Skype, Windows Live Messenger, Yahoo! Messenger, mIRC, Trillian, MyChat, LingoWare, Chit Chat For Facebook, Nimbuzz, Facebook Messenger, Microsoft Communicator 2007, Facemoods, Gaim, LAN Chat Enterprise, OpenTalk, TurboIRC, WinSent Messenger, Pink Notes Plus, fTalk, XChat, ooVoo, TweetDeck, Pidgin Instant Messenger,NateOn Messenger, QQ International , Twhirl, Daum MyPeople
Cloud Services / File Sharing	Google Drive Client, iCloud, Dropbox, Microsoft SkyDrive, eMule, Kazaa, Shareaza, Morpheus, eDonkey, DC++, BitTorrent, Azureus, BitComet, uTorrent, iMesh, Daum Cloud, KT Olleh uCloud, Naver NDrive, Microsoft Skydrive client, Limewire, FTP Command, ownCloud client, Pogoplug Backup, Pruna P2P, Sendspace, Evernote, FileCloud Sync client
Social Media/Others	InfraRecorder, iTunes, Nokia PC Suite 2008 / 2011, Samsung Kies, Sony Ericsson PC Companion, TeamViewer, HTC Sync for Android phones, Total Commander, LogMeIn, EasyLock, GoToMeeting, Windows DVD Maker, FileZilla, ALFTP, GoToMeeting

The last step in defining a new policy consists in selecting the content to detect from the three separate tabs for Content Filters.

The File Type Filter contains a list of supported file types grouped in six categories:

- Graphic Files: JPEG, PNG, GIF, ICO, BMP, TIFF, EPS, CorelDraw etc.
- Office Files: Word (DOC, DOCX), Excel (XLS, XLSX), PowerPoint (PPT, PPTX), PDF, Infopath (XSN), RTF, OneNote (ONE), Outlook (PST, OST) etc.
- Archive Files: ZIP, 7z, RAR, ACE, TAR etc.
- Programming Files: C, CPP, JAVA, PY, SH, CSH, BAT, CMD, PAS, XML, DTD TEX, F etc.
- Media Files: MP3, M4A, WAV, WMA, AVI, AIF, M3U, MPA etc.
- Other Files: EXE, SYS, DLL, SO etc.

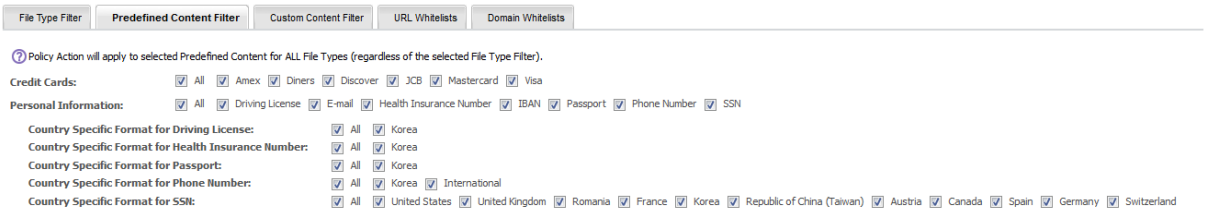
For each category, the most common file types are displayed. To be able to view and select more file types, click on the More File Types option at the end of each file type enumeration.


File Type Filter
Predefined Content Filter
Custom Content Filter
URL Whitelists
Domain Whitelists
Policy Action will apply to selected File Types
Graphic Files: All JPEG PNG GIF ICO BMP TIFF More File Types
Office Files: All Word Excel PowerPoint PDF Infopath Outlook More File Types
Archive Files: All ZIP ZIP/password 7z RAR ACE TAR More File Types
Programming Files: All c, cpp, java py sh, csh bat, cmd pas xml, dtd More File Types
Other Files: All AutoCAD files Text files DRM Files exe, sys, dll so Unidentified More File Types
Media Files: All mov mp3 m4a wav wma avi More File Types
Save
Back
Delete

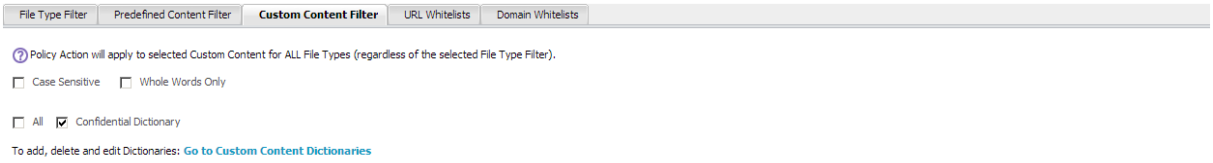
Note!

As many files (e.g. Programming Files) are actually TXT files, we recommend more precaution when selecting this file type to avoid any undesired effects.

The "Predefined Content Filter" displays a list of predefined items to detect, from credit card information to Personal Identifiable Information. The Content Aware Protection module offers the option of Localization, meaning that you can select specific formats for a list of countries for information such as Driving License, ID, Phone Number and Social Security Number. By leaving unchecked this option, all formats will be detected by the Content Aware Protection agent.


File Type Filter
Predefined Content Filter
Custom Content Filter
URL Whitelists
Domain Whitelists
Policy Action will apply to selected Predefined Content for ALL File Types (regardless of the selected File Type Filter).
Credit Cards: All Amex Diners Discover JCB Mastercard Visa
Personal Information: All Driving License E-mail Health Insurance Number IBAN Passport Phone Number SSN
Country Specific Format for Driving License: All Korea
Country Specific Format for Health Insurance Number: All Korea
Country Specific Format for Passport: All Korea
Country Specific Format for Phone Number: All Korea International
Country Specific Format for SSN: All United States United Kingdom Romania France Korea Republic of China (Taiwan) Austria Canada Spain Germany Switzerland

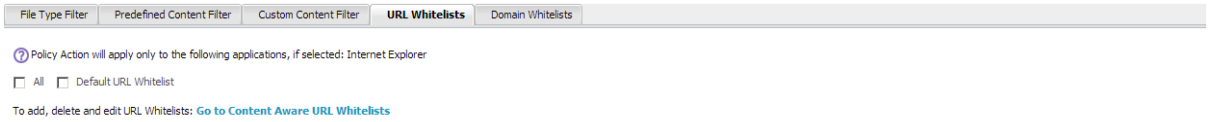
The "Custom Content Filter" displays a list of Content Aware dictionaries. By selecting one or more dictionaries, the Content Aware Protection agent will detect any occurrence of one, more or all terms contained in the Dictionary list.


File Type Filter
Predefined Content Filter
Custom Content Filter
URL Whitelists
Domain Whitelists
Policy Action will apply to selected Custom Content for ALL File Types (regardless of the selected File Type Filter).
Case Sensitive
Whole Words Only
All
Confidential Dictionary
To add, delete and edit Dictionaries: Go to Custom Content Dictionaries

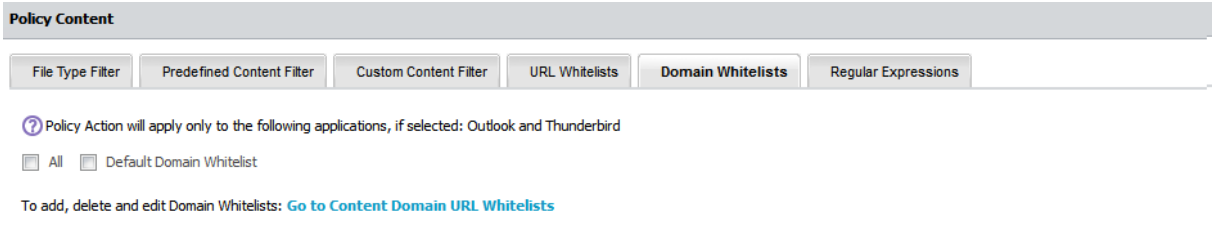
By checking the Case Sensitive option, the agent can differentiate the uppercase and lowercase letters when inspecting the content.

If the Whole Words Only option is marked, terms from the inspected content are detected only if they are an identical match with the ones that appear in the dictionary (e.g. „age" is in the Dictionary; variations like „aged", „agent", „agency" etc. won´t be reported/blocked).

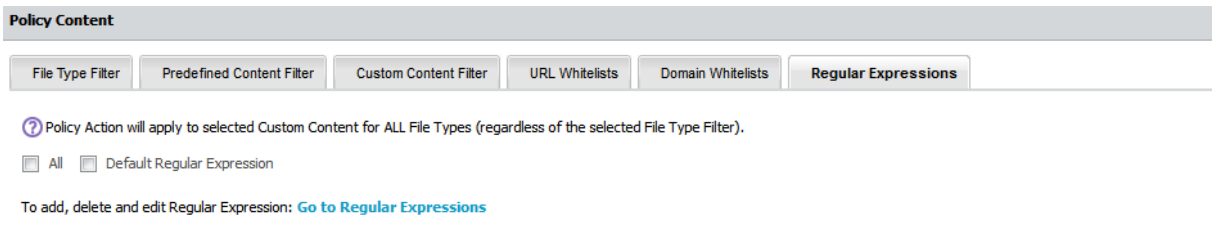
The "URL Whitelist" displays a list of URL whitelists. By selecting one or more whitelists, the Content Aware Protection agent will not scan uploads or attachments to the web addresses present in the whitelists. Whitelisting works for Internet Explorer.


File Type Filter
Predefined Content Filter
Custom Content Filter
URL Whitelists
Domain Whitelists
Policy Action will apply only to the following applications, if selected: Internet Explorer
All
Default URL Whitelist
To add, delete and edit URL Whitelists: Go to Content Aware URL Whitelists

The "Domain Whitelist" displays a list of domain whitelists. By selecting one or more whitelists, the Content Aware Protection agent will not scan mails sent to the recipients or domains present in the whitelists. Whitelisting works for Microsoft Outlook and Mozilla Thunderbird.


Policy Content
File Type Filter
Predefined Content Filter
Custom Content Filter
URL Whitelists
Domain Whitelists
Regular Expressions
Policy Action will apply only to the following applications, if selected: Outlook and Thunderbird
All
Default Domain Whitelist
To add, delete and edit Domain Whitelists: Go to Content Domain URL Whitelists

The "Regular Expressions" shows the list of the created regular expressions and the administrator can select up to five (5) expressions.


Policy Content
File Type Filter
Predefined Content Filter
Custom Content Filter
URL Whitelists
Domain Whitelists
Regular Expressions
Policy Action will apply to selected Custom Content for ALL File Types (regardless of the selected File Type Filter).
All
Default Regular Expression
To add, delete and edit Regular Expression: Go to Regular Expressions

Once a policy is created, it will be displayed inside the Policies List. To enforce a content aware policy inside the network, one must select the specific policy that they want to apply by clicking on it and check the corresponding boxes to the network entity on which they want to apply the content rules. If a Content Aware Policy was already enforced on a computer, user or group, when clicking on it, the corresponding network entities on which it was applied will be highlighted.

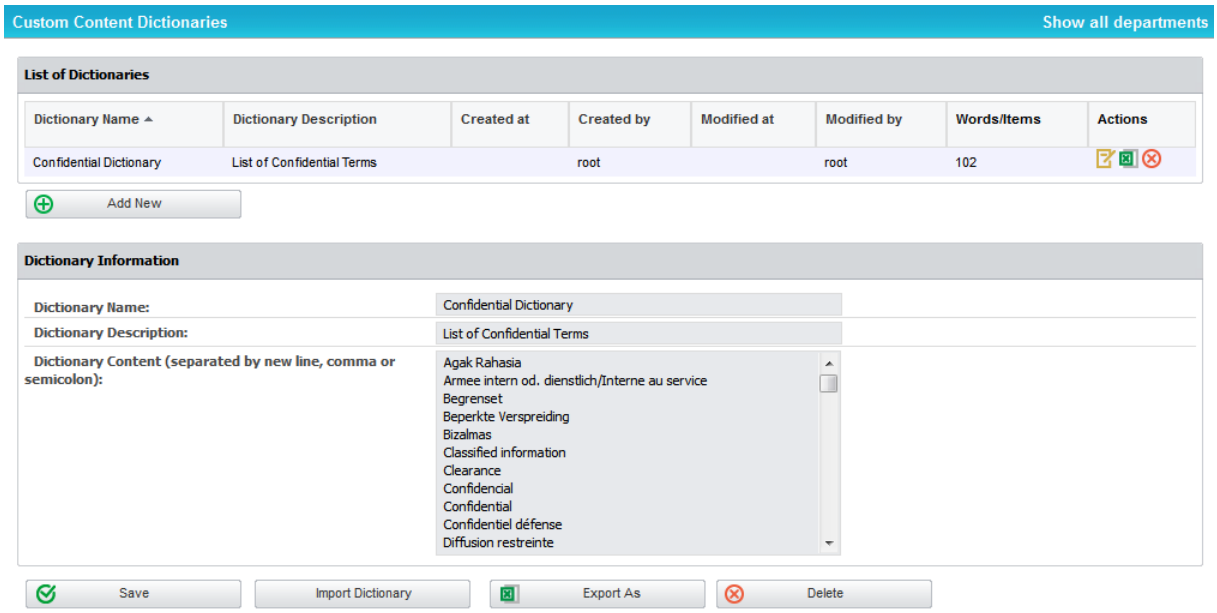
The administrator can be notified of each occurrence of an event described in a newly created policy by setting up a Content Aware alert for that specific policy from Alerts > Content Aware Alerts.

6.2. Custom Content Dictionaries

Custom Content Dictionaries are custom defined lists of terms and expressions to be detected as sensitive content by My Endpoint Protector. The list of custom content dictionaries is available under Content Aware Protection -> Custom Content Dictionaries.

The available actions for each dictionary are: **Edit**, **Export Dictionary** and **Delete**.

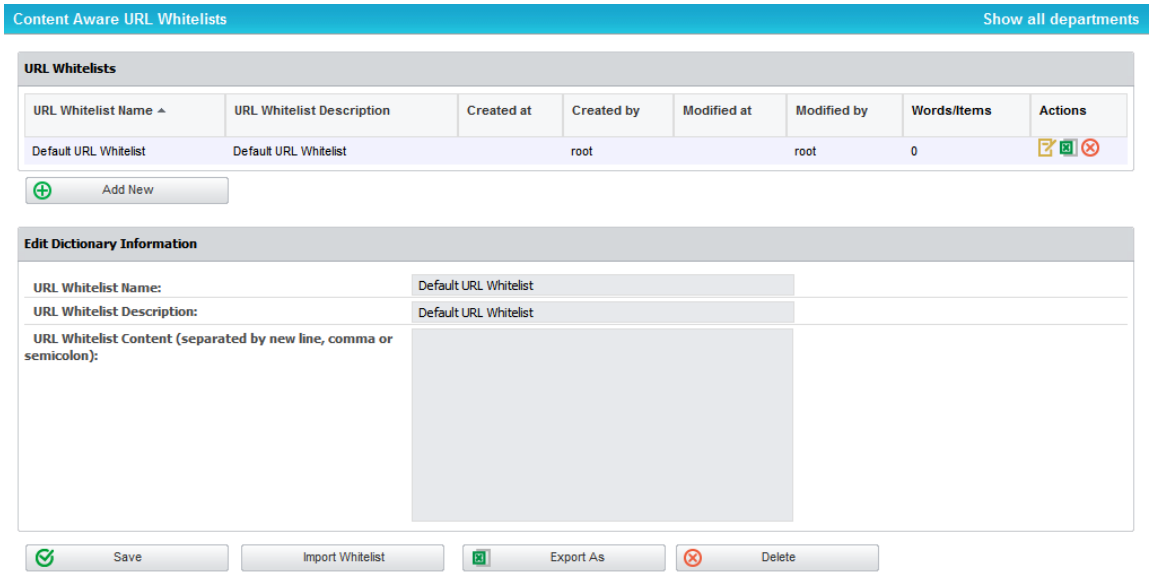
One can create a new dictionary by clicking on the "Add New" button. To populate the content of a newly created dictionary, items of at least three characters might be entered either manually separated by comma, semicolon or new line or directly imported from an Excel file by pressing the Import Dictionary button. An example of a Custom Content Dictionary populated with Financial Terms is shown below:



Once a new dictionary is created, it will be automatically displayed inside the Custom Content tab when creating a new or editing an existing Content Aware Policy. The Content Aware Protection module comes with a predefined set of dictionaries.

6.3. Content Aware URL Whitelists

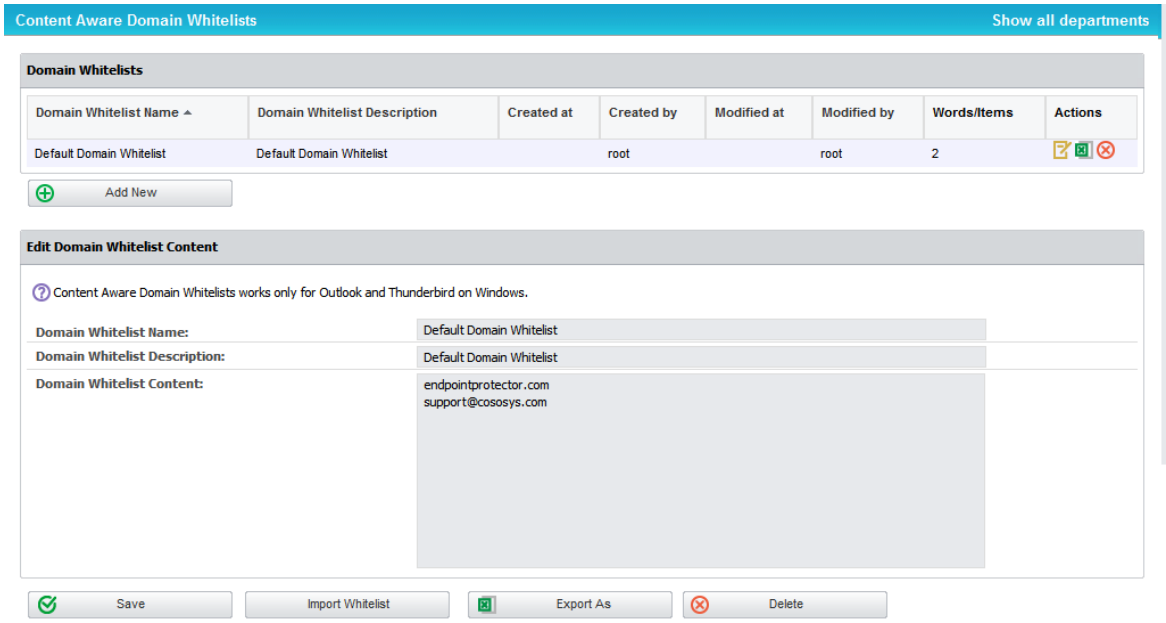
URL Whitelists are custom defined lists of web addresses where uploading of confidential information will be allowed by My Endpoint Protector. This feature works on Internet Explorer.



Once a new URL whitelist is added, it will be automatically displayed inside the URL Whitelists tab.

6.4. Content Aware Domain Whitelists

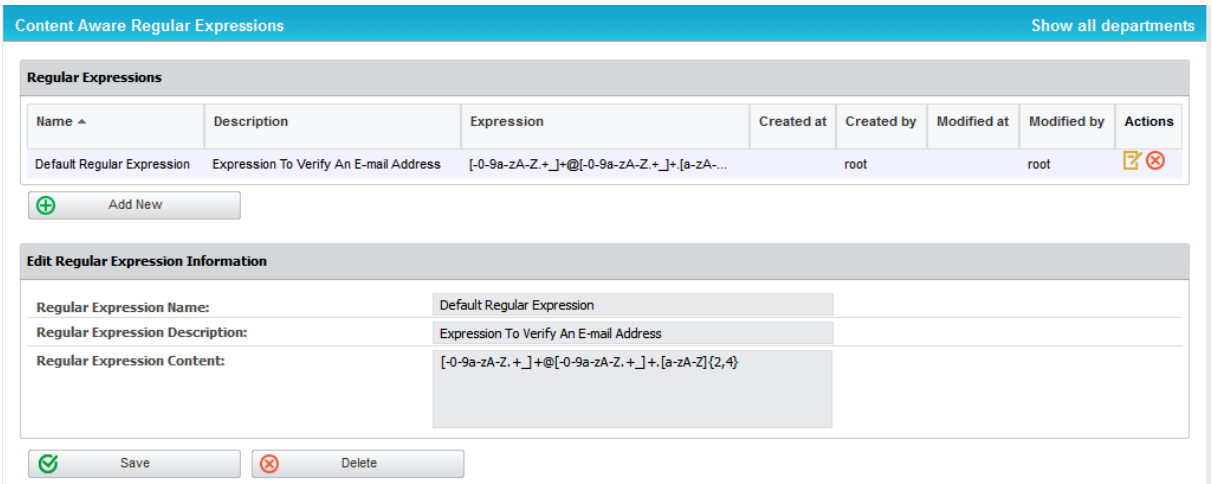
Domain Whitelists are custom defined e-mail addresses to which sending of confidential information will be allowed by My Endpoint Protector .This feature works on Microsoft Outlook and Mozilla Thunderbird.



Once a new domain whitelist is added, it will be automatically displayed inside the Domain Whitelists tab.

6.5. Content Aware Regex (Regular Expressions)

By definition, Regular Expressions are sequences of characters that form a search pattern, mainly for use in pattern matching with strings. An administrator can create a regular expression in order to find a certain recurrence in the data that is transferred across the protected network.



Example that matches an e-mail: **[-0-9a-zA-Z.+_]+@[-0-9a-zA-Z.+_]+\.[a-zA-Z]{2,4}**

Example that matches an IP: **(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)(\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)){3}**

Note! If possible, avoid using Regular Expressions, as their complexity typically increases the resources usage.Using a large number of regular expressions as filtering criteria typically increases CPU usage. Also, improper regular expressions or improper use can have negative implications.

This feature is provided "as is" and requires advanced knowledge of the Regular Expression syntax.
The regular expressions feature is provided with no direct support and it is the responsibility of the customers to learn and implement regular expressions and to thoroughly test.

6.6. How Content Aware Protection works for monitored Applications / Online Services

The following table shows a list of actions and content that are screened/inspected or left unscreened/uninspected by the Content Aware Protection feature.

APPLICATION	SCREENED	NOT SCREENED
Web Browsers	Uploaded Files Webmail Attachments	Webpage Content Downloaded Content Blog Posts
E-MAIL Clients	File Attachments Microsoft Outlook E-MAIL Content Microsoft Outlook Forwarded and Saved Attachments Microsoft Outlook E-mailed directly from Windows Explorer Microsoft Outlook Copied Attachments from one E-MAIL to another Mozilla Thunderbird E-MAIL Content	E-MAIL Content for other E-MAIL Services Forwarded Attachments Saved Attachments Attachments e-mailed directly from Windows Explorer Copied Attachments from one E-MAIL to another
Instant Messaging	File Transfers Shared Picture Files	IM Message Content Sent Files

File Sharing	File Uploads	Saved Files
Social Media/Other	File Transfers	Blog Posts

*Other limitations may apply.

7. Offline Temporary Password

7.1. Device Offline Temporary Password

This module allows the user of the commercial My Endpoint Protector account to generate a temporary password for a specific device on a client user computer. It can be used when there is no network connection between the client computer and the Server.

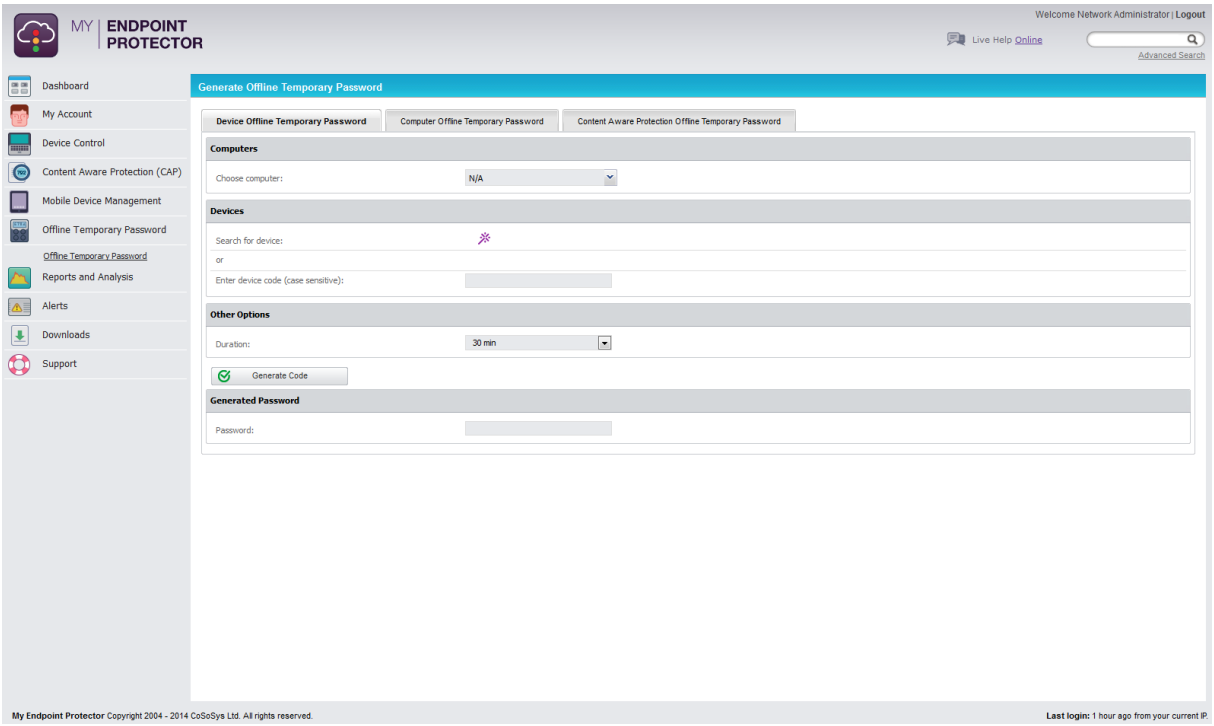
Note!

Once a device is temporarily authorized, any other rights/settings saved afterwards for this device will not take immediate effect, until the time period is passed and the connection with the Server is re-established.

A password is unique for a certain device and time period. In conclusion, the same password cannot be used for a different device or for the same device twice.

The password will give permission to the device for the specified amount of time.

The time intervals which can be selected are: 30 minutes, 1 hour, 2 hours, 4 hours, 8 hours, 1 day, 2 days, 5 days, 14 days and 30 days.

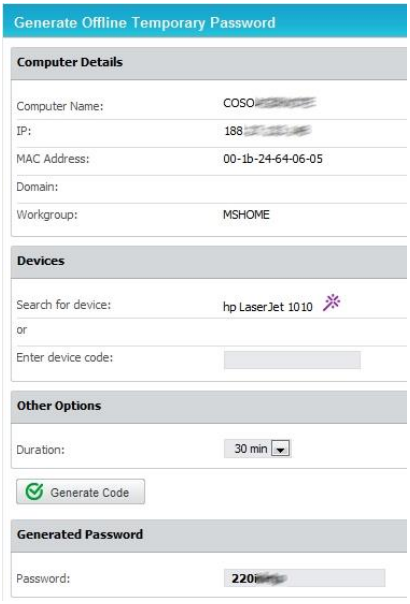


The administrator can either search for an existing device using the search wizard

or, in case the device is not already in the database, he can introduce the device code communicated by the client user (explained in bellow paragraph).

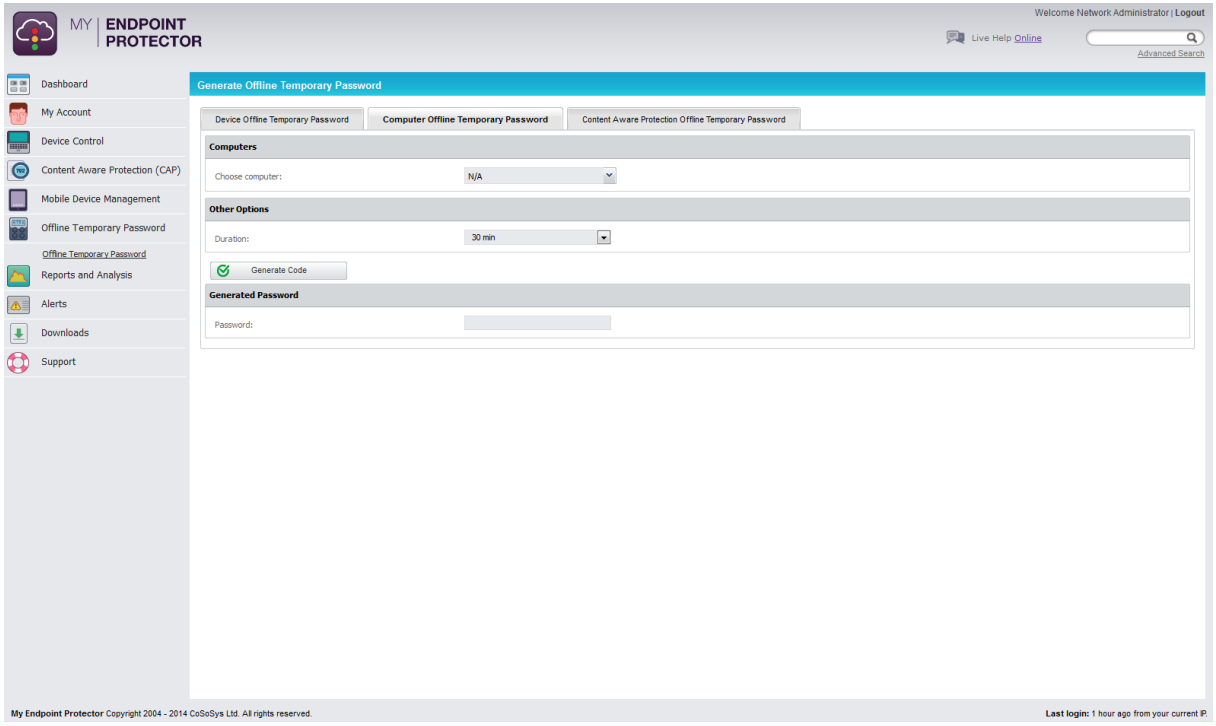
After selecting the duration, the password will be generated by clicking "Generate Code" button.

Another way to generate a password is by selecting a client computer from Device Control > Computers list, with the action "Offline Temporary Password".



The obtained password will be communicated to the user for temporarily allowing his specific device as explained below.

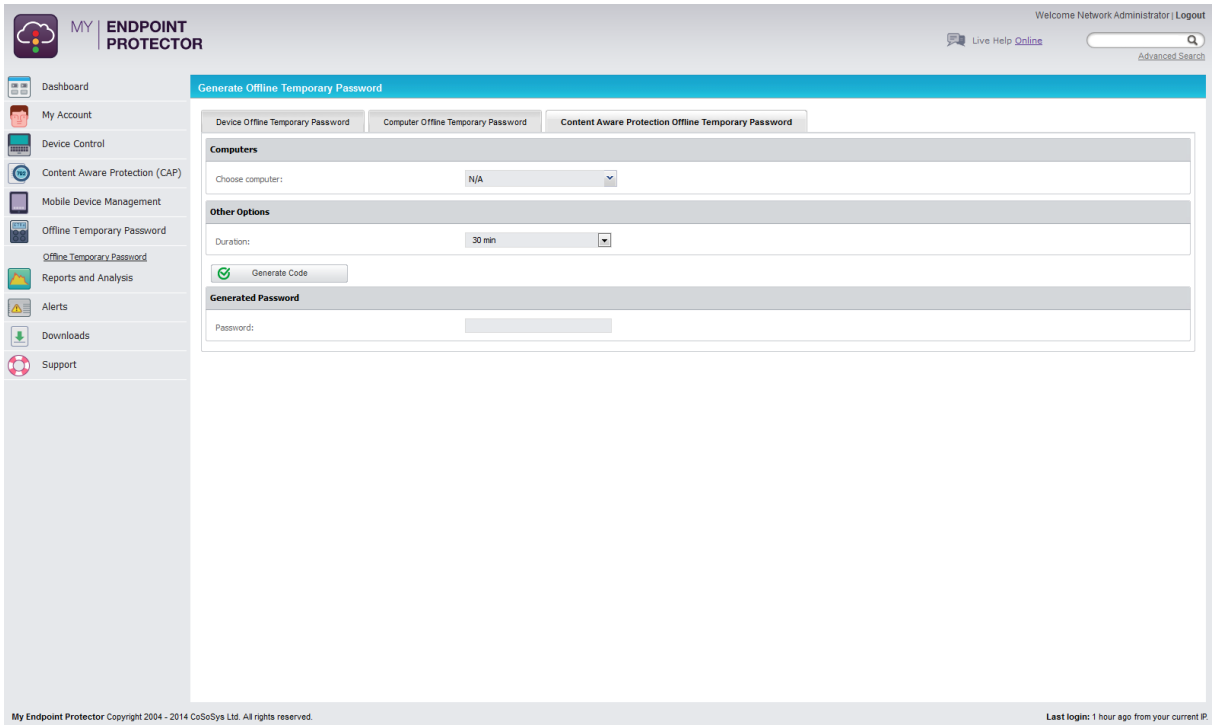
7.2. Computer Offline Temporary Password



The administrator can allow the use of all the endpoints on an offline computer. He does this by generating a Computer Offline Temporary Password. After selecting the computer and duration, the password will be generated by clicking on the "Generate Code" button. The obtained password will be communicated to the user for temporarily allowing the use of all the endpoints as explained in paragraph 5.5.

7.3. Content Aware Protection Offline Temporary Password

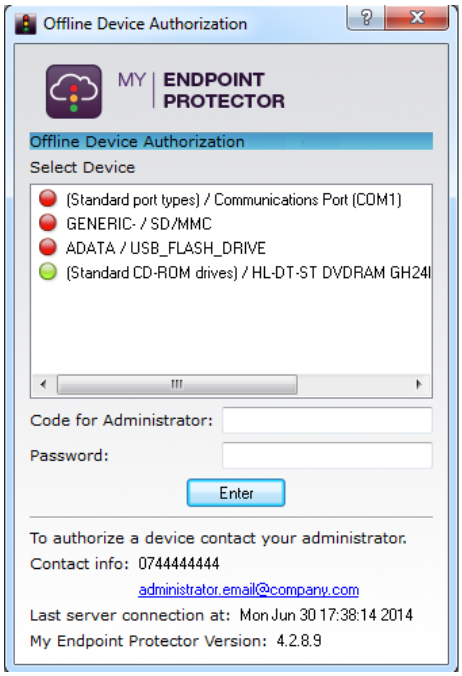
The administrator can allow the transfer of sensitive data on an offline computer. He does this by generating a Content Aware Protection Offline Temporary Password. After selecting the computer and duration, the password will be generated by clicking on "Generate Code" button. The obtained password will be communicated to the user for temporarily allowing transfer of sensitive data as explained in paragraph 5.5.



7.4. Offline Device, Computer and Content Aware Protection Authorization

In order to select a device and enter a password, the user needs to click on the My Endpoint Protector icon from the system tray.

The user will select the device from the list and contact the administrator at the displayed contact information.



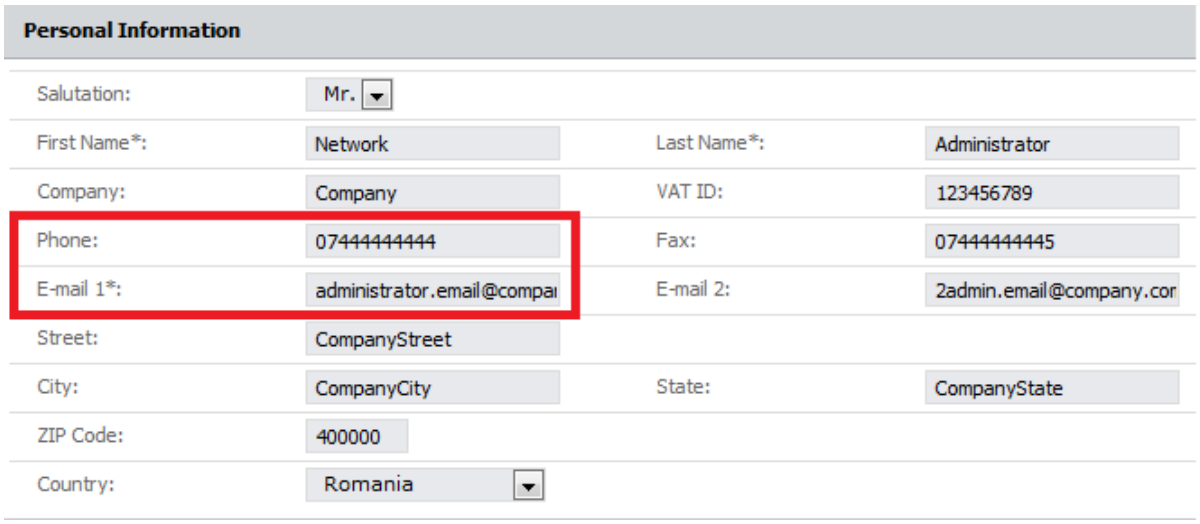
The user will tell the administrator the code for the device and the administrator will tell the user the password, after generating it on the Server (see above paragraph for password generation).

The password will be inserted in the corresponding field and applied by clicking "Enter".

For Computer and Content Aware Protection authorization the administrator will tell the user the password he previously generated.The user will simply enter it in the „Password" field and apply it by clicking „Enter".

7.5. Setting the Administrator Contact Information

The Administrator contact information can be edited under "My Account" > "Profile Details" module, at the "Personal Information" panel.

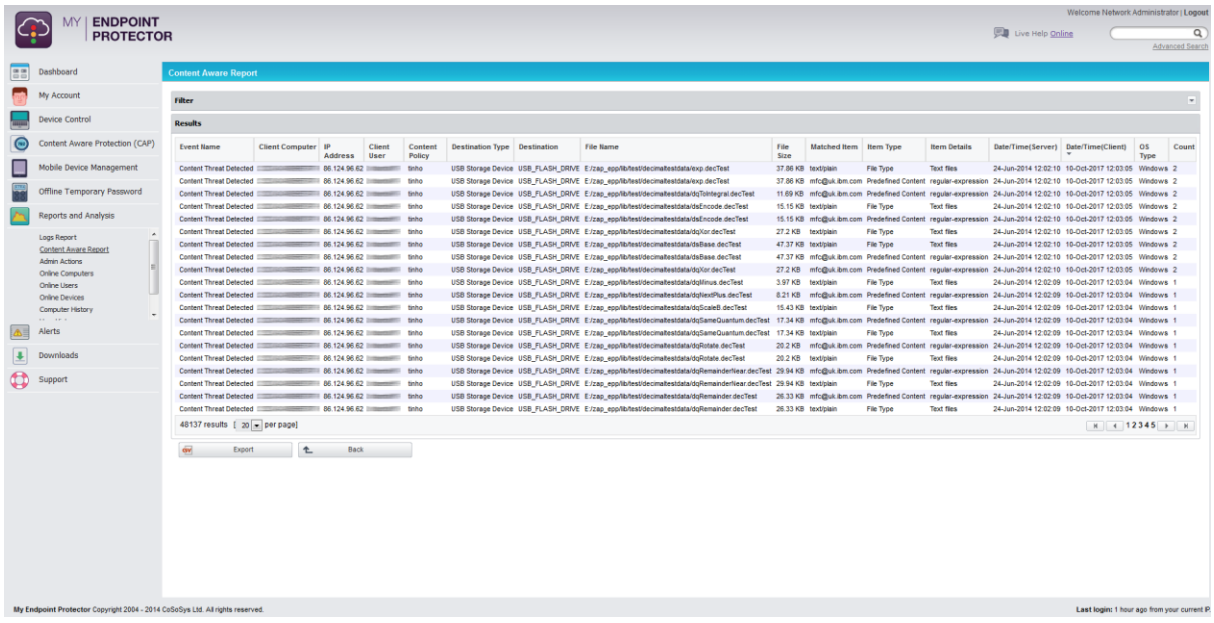


8. Reports and Analysis

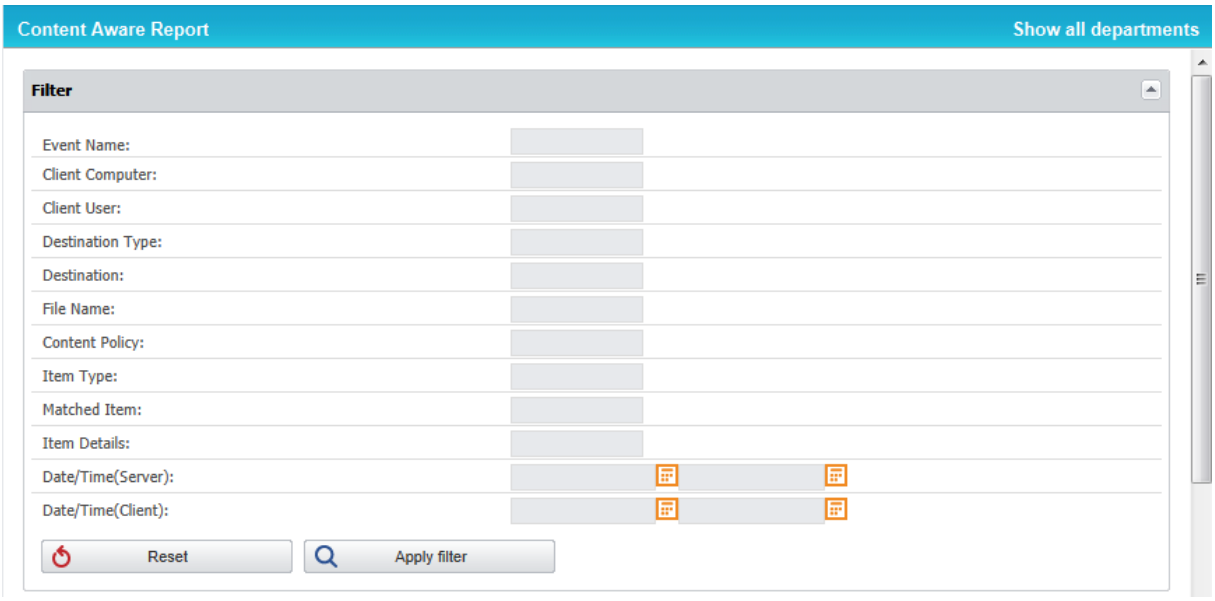
This module is designed to offer you, the administrator feedback regarding system functionality and information related to devices, users and computers in the entire system.

8.1. Content Aware Report

This module provides detailed logs of all Content Aware activity. It allows the administrator to see exactly what data incidents were detected corresponding to the Content Aware Policies applied and at what time. This information also contains the computer name, user and transfer destination type, the action taken and the file inspected. The included granular filter is designed to make finding information quick and easy.

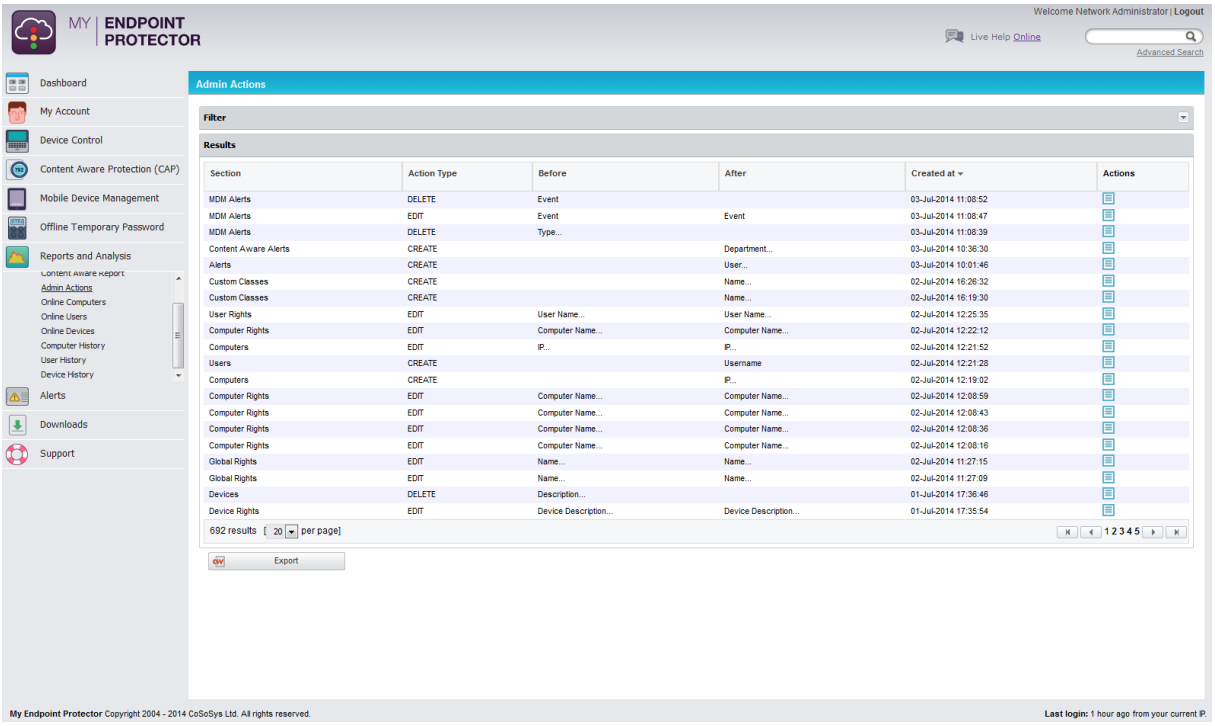


The administrator has the possibility of exporting both the search results and the entire log report as a .CSV file, which can later be printed out for detailed auditing.



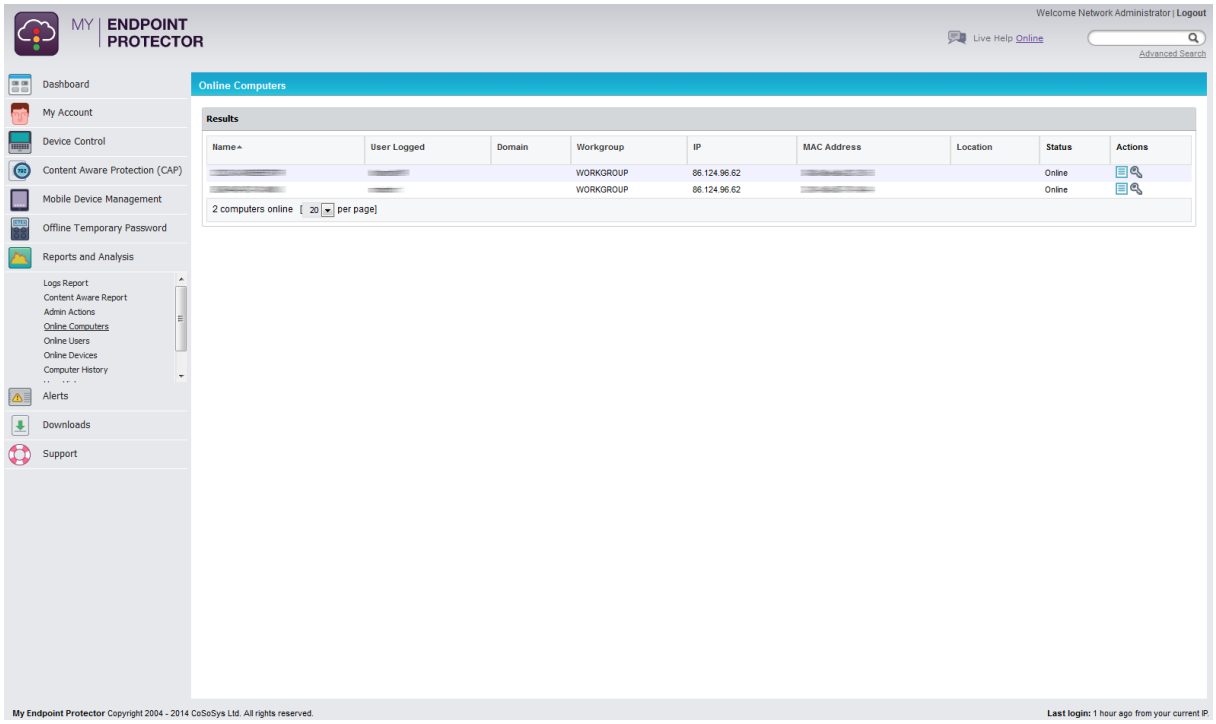
8.2. Admin Actions

Every important action performed by administrators in the interface is recorded. Clicking the "view details" button will open the "Admin Actions Details" page where further details about the specific event is shown, with the status of the modified feature before and after the change took place.



The logs can be exported in a .csv file, while the filter can help find the desired information quickly and easily.

8.3. Online Computers



Offers real time* monitoring of the client computers registered on the system, which have an established connection with the server.

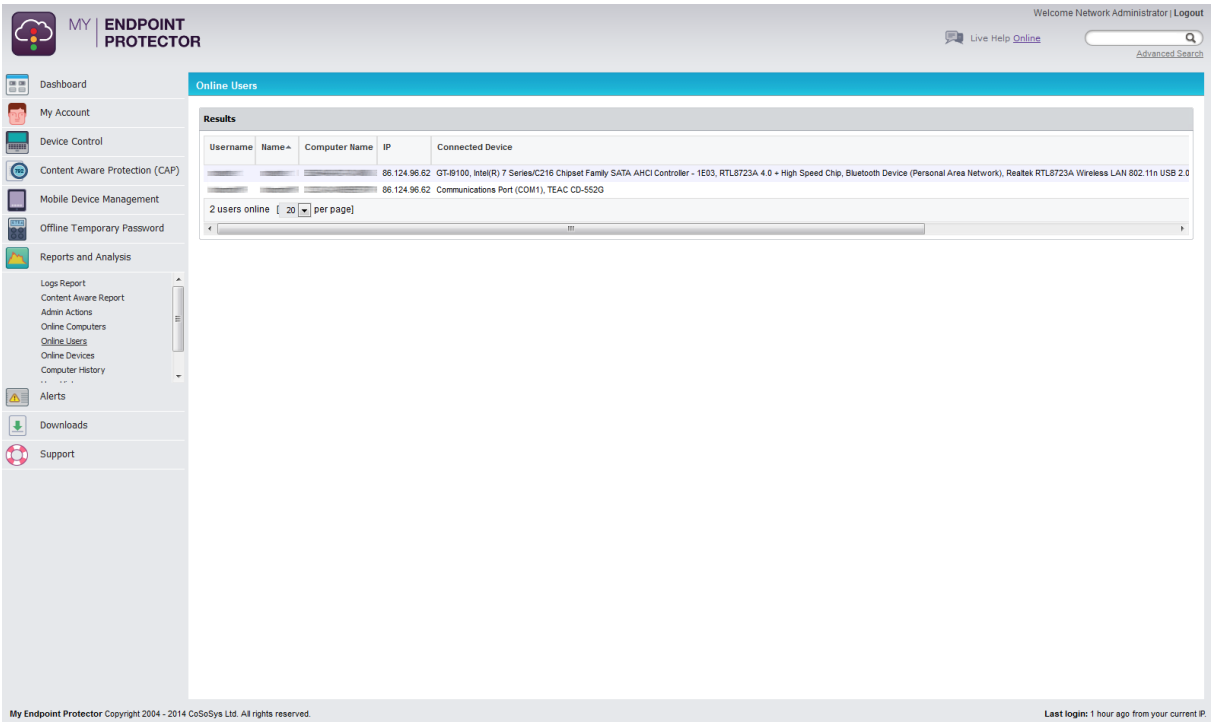
*depends on the Refresh Interval; if the Refresh Interval for computer X is 1 minute, than the computer X was communicating with the server in the last 1 minute.

The administrator has the possibility of accessing the log for a certain computer by pressing the “List” action button.

Pressing this button will take you to the logs report, where it will only display the actions of that specific computer for which the button was pushed.

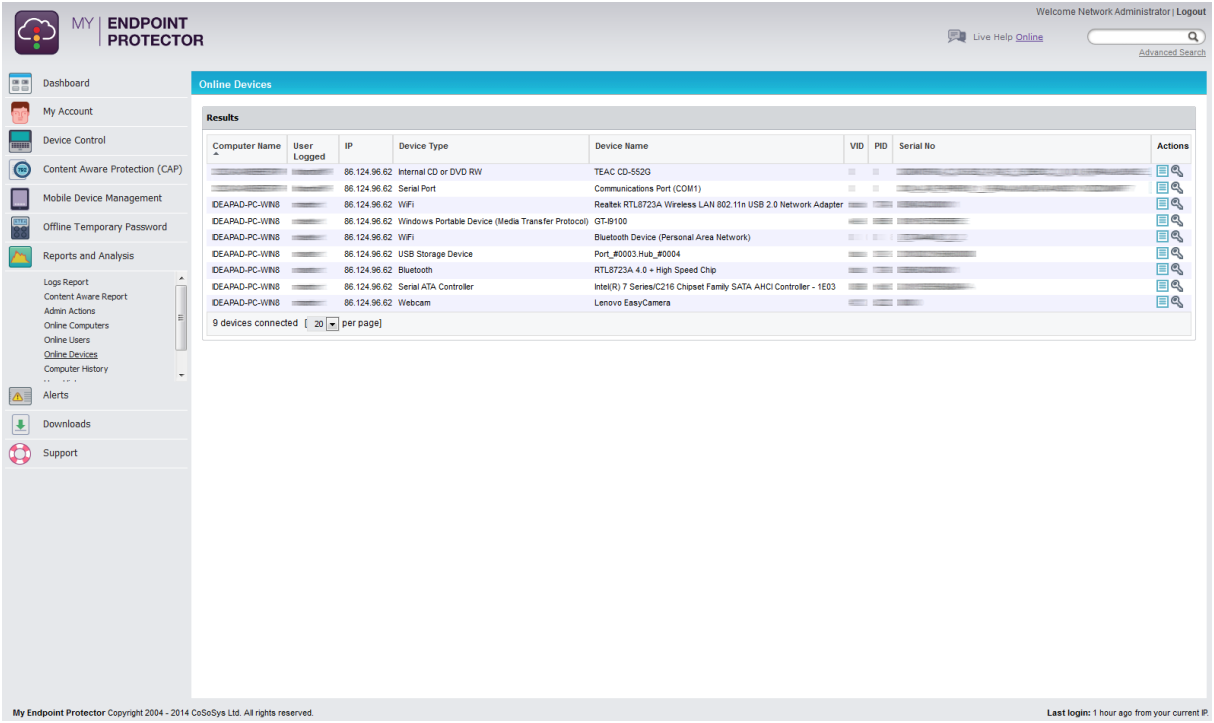
8.4. Online Users

Shows a list of users that are connected to the My Endpoint Protector Server in real time.



8.5. Online Devices

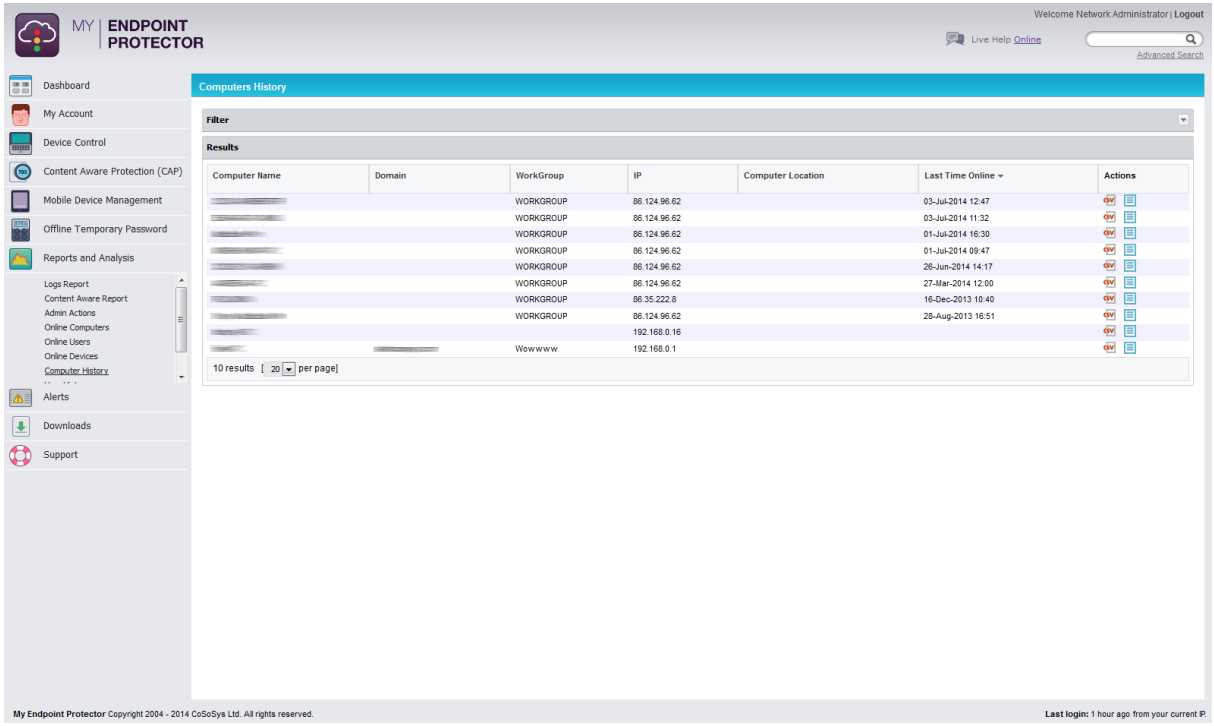
Offers information regarding the devices connected to the computers on the system.



The administrator can see which devices are connected to what computers and also the client user who is accessing them. The administrator can also use the action buttons “View Log” and “Manage Rights” to quickly administer the device.

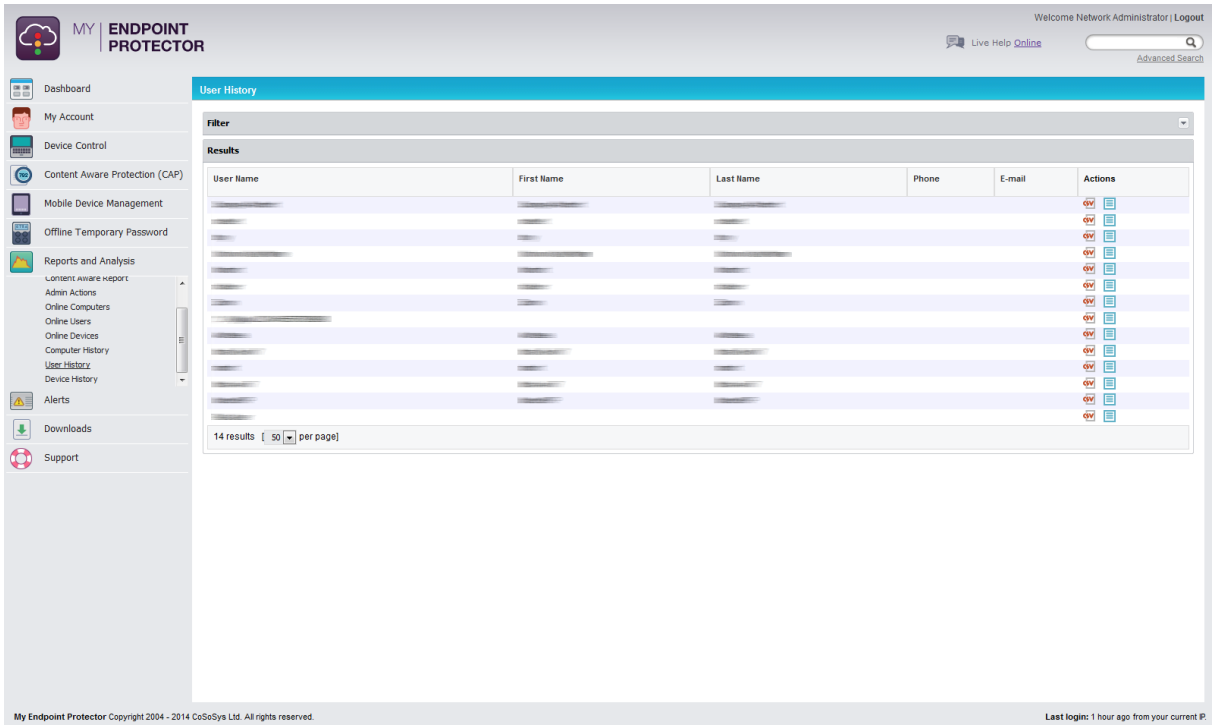
8.6. Computer History

This module shows all computers that were at least once connected to the server. With the help of the “Export” button the logs can be saved to a .csv file, while pressing the “View Machine log” will show the Logs Report page filtered for the respective Computer.



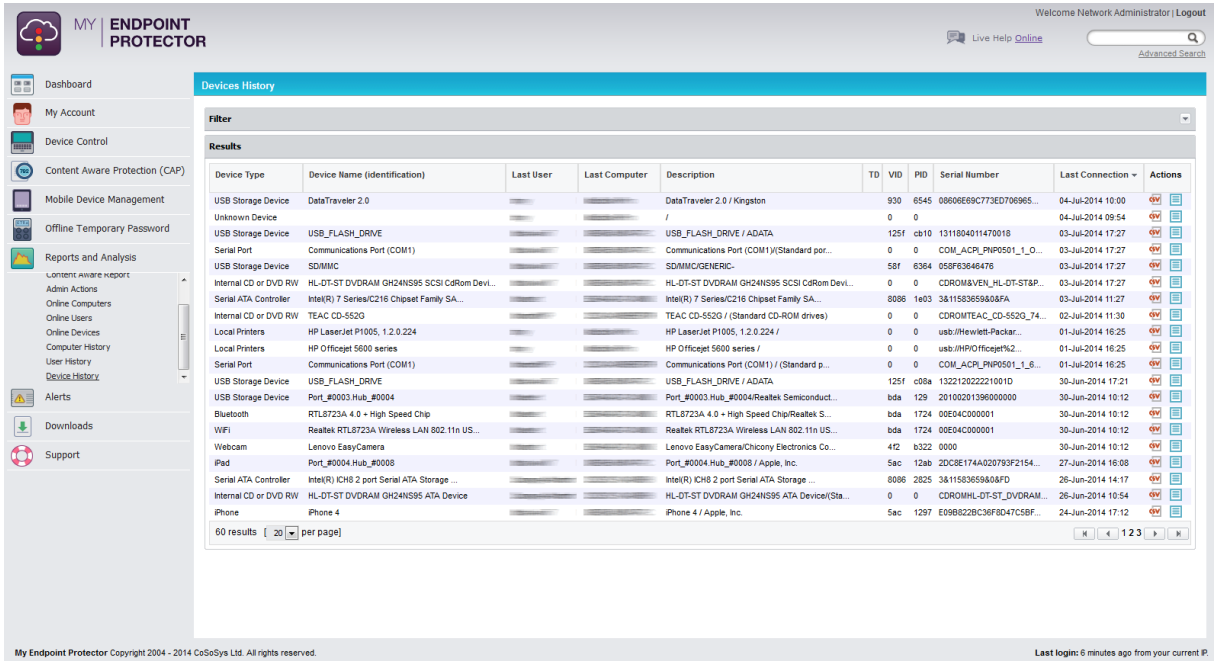
8.7. User History

This module shows all users that were at least once connected to the server. With the help of the “Export” button the logs can be saved to a .csv file, while pressing the “View User log” will show the Logs Report page filtered for the respective User.



8.8. Device History

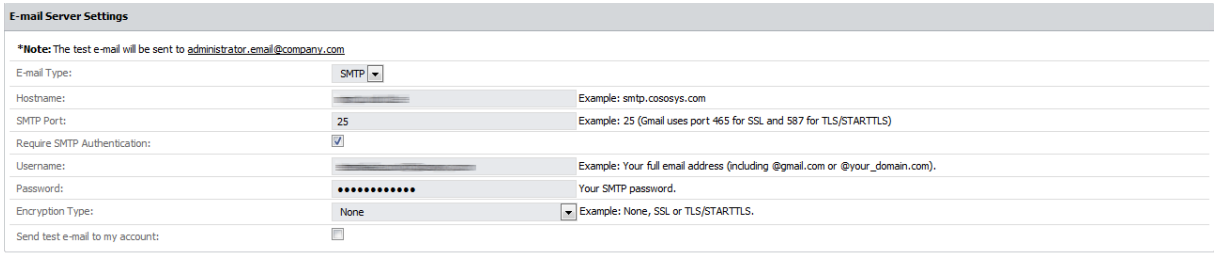
Similar to Computer and User history, all devices that were at least once connected to the server can be found here. Logs can be exported to a .csv file by pressing the “Export” button, while “View Device Log” will show the Logs Report page filtered for the respective device.



9. Alerts

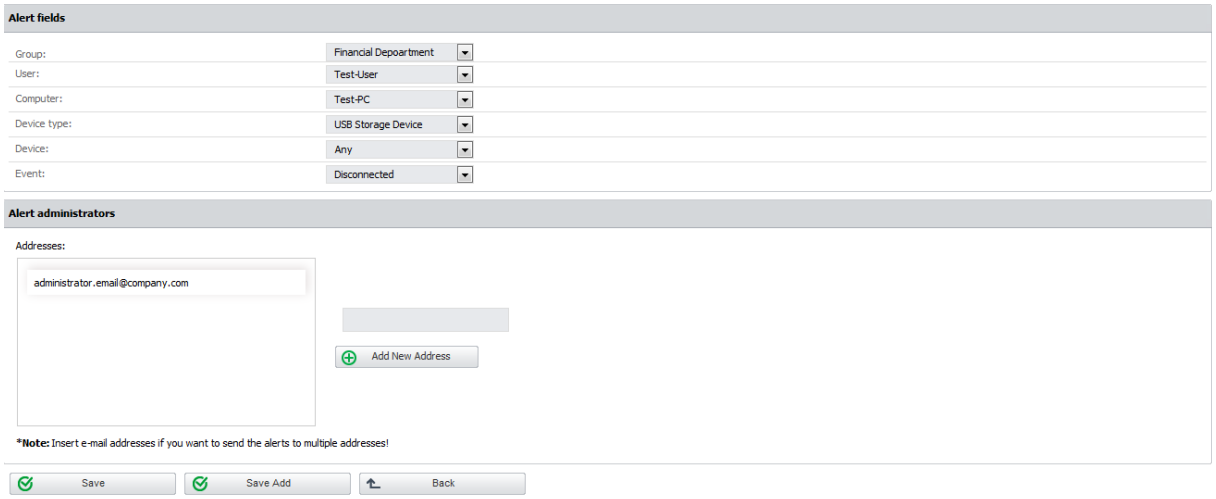
My Endpoint Protector allows you to set notifications (Alerts) for Devices, Computers, Groups and Users making monitoring them easier. An Alert will trigger an e-mail that will be sent to the selected administrator(s), which are intended to receive the alerts. You can set up device related activity alerts in the System Alerts-> Define System Alerts module in Endpoint Protector. The Define Content Aware Alerts option will allow administrators to set special alerts for sensitive content detection and transfer blocking.

Before you can create an E-MAIL alert, you must configure the server host and provide a user name and password to that mail server. You can do that by accessing "Global Settings" in the "Device Control" module.



You can also verify if your settings are correct by checking the box next to "Send test E-MAIL to my account". The test E-MAIL and the Alerts will be sent to the E-MAIL address configured in the "My Account" > "Profile Details" > "E-Mail 1*" field.

Click "Create" to start creating the first alert.



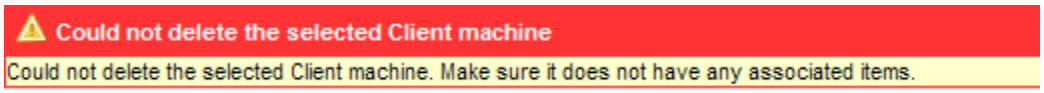
Then select the Group, Client, Computer, Device type or Device, - depending if you mean a single device or all devices of a certain type, and the event that will trigger the notification.

You can also select one or more users to receive the same notification(s). This is useful in case there is more than one administrator for My Endpoint Protector.

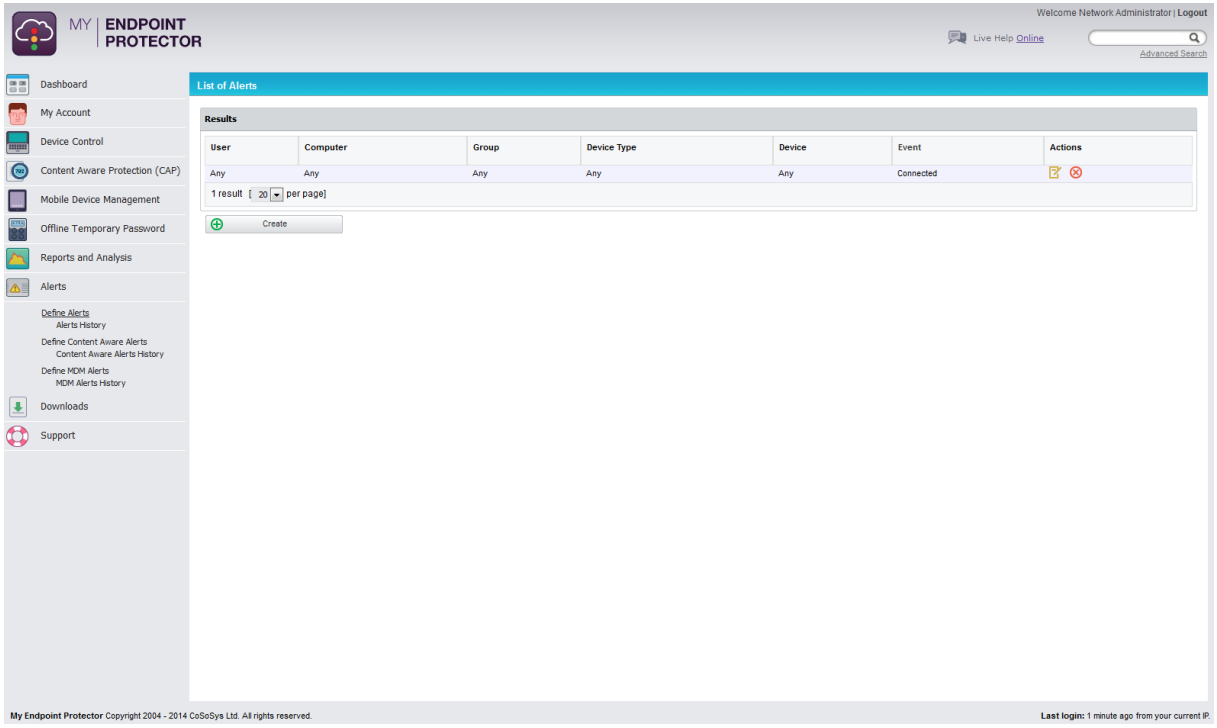
Example: if you want to be notified when a certain device is connected to a certain computer you must set up an alert choosing the specific device and computer that you wish to be notified of and selecting the "Connected" event from the events list.

The "Client" and "Group" fields do not influence the triggering of the alert, so there is no need to fill them out. Setting up a value for the "Group" field means that the alert will be triggered when the selected event occurs for any clients or computers in that group.

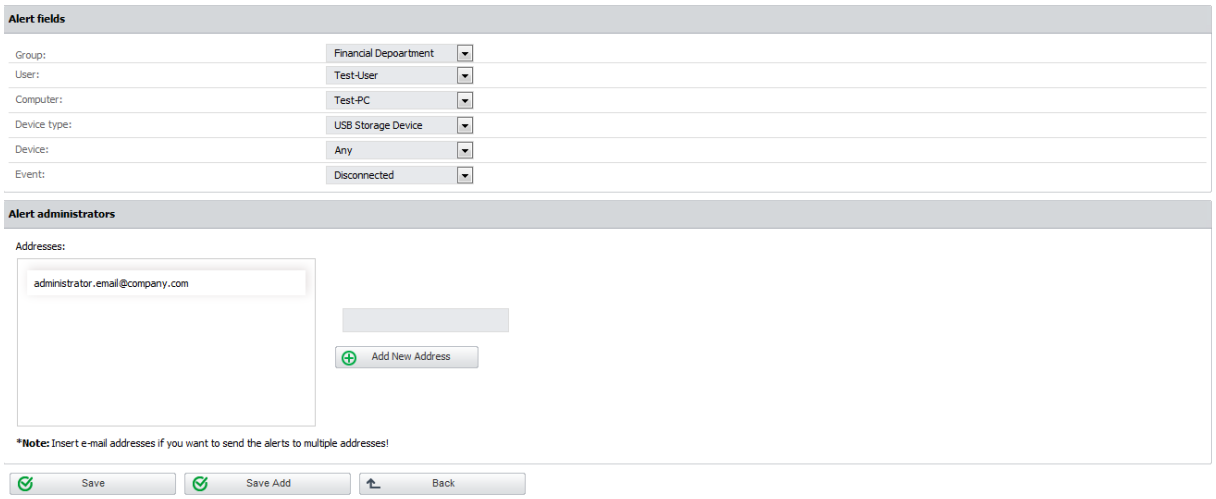
If you try deleting any items (Users, Groups, Computers etc.) that have been used in setting up an alert, you will receive a notification, and you will not be able to delete them.


Could not delete the selected Client machine
Could not delete the selected Client machine. Make sure it does not have any associated items.

9.1. Define Alerts



To create a new alert, go to "Define Alerts" and click "Create".



Then select the Group, User, Computer, Device type or Device, - depending if you mean a single device or all devices of a certain type-, and the event that will trigger the alert. You can add up to five (5) E-MAIL addresses to which the alert(s) will be sent.

Example: if you want to be notified when a certain device is connected to a certain computer you must set up an alert choosing the specific device and computer that you wish to be notified of and selecting the "Connected" event from the events list.

In this case, the "Client" and "Group" fields do not influence the triggering of the alert so there is no need to fill them out. Setting up a value for the "Group" field means that the alert will be triggered when the selected event occurs for any clients or computers in that group.

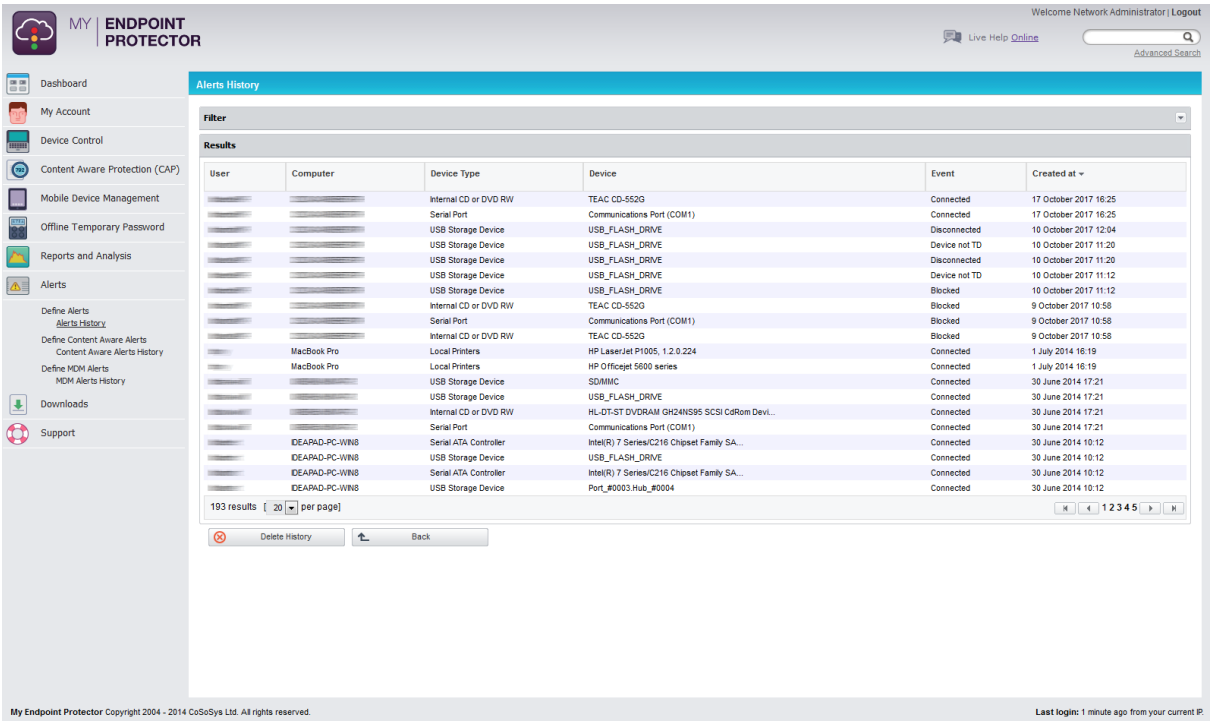
If you wish to delete any entity (Users, Groups, Computers etc.) that have been used in setting up an alert, you will receive a notification, and you will not be able to delete them.

Could not delete the selected Client machine
Could not delete the selected Client machine. Make sure it does not have any associated items.

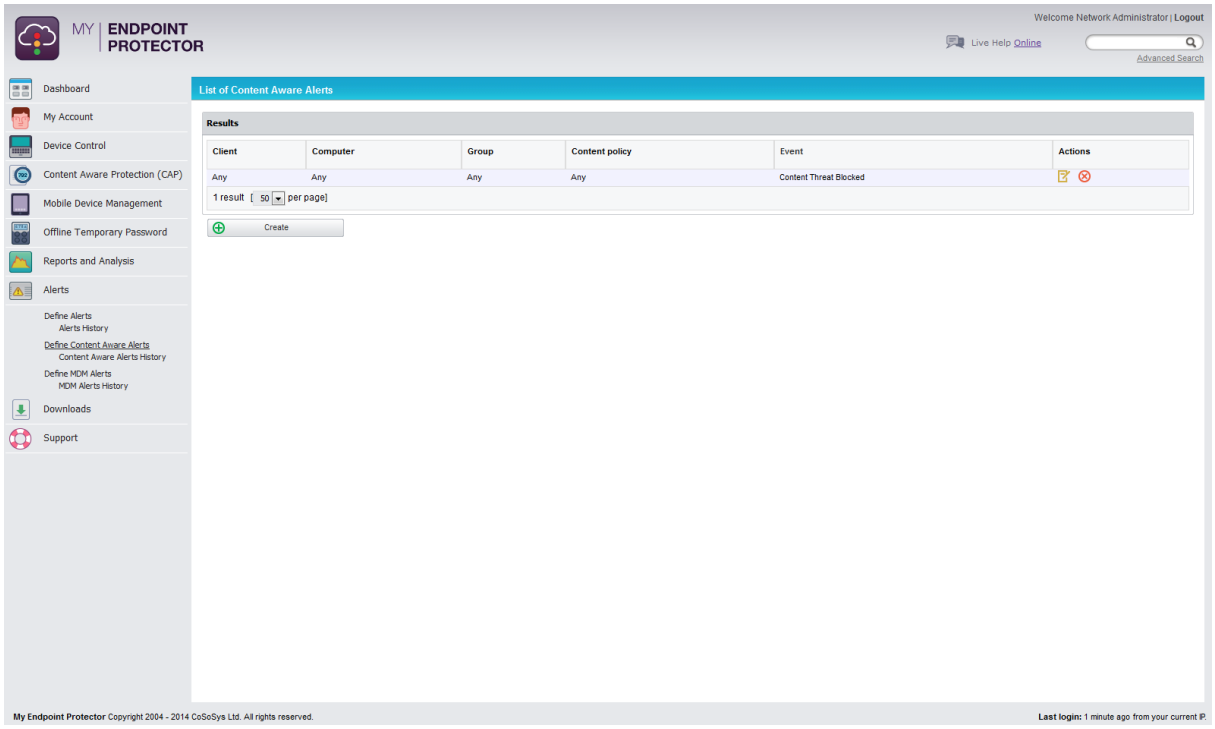
In order to be able to delete them, the administrator must either edit the alert not to contain the respective entity or delete the alert.

9.2. Alerts History

A history of the alerts is kept in this tab for later auditing. Each event that triggers an alert will be saved here. Administrators can search for data more easily with the implemented filter, while if not needed anymore the logs can be deleted from the "Delete History" button.



9.3. Define Content Aware Alerts



To create a new Content Aware Alert corresponding to the policies defined in the Content Aware Protection module, go to Define Content Aware Alerts submenu option and click “Create”.

Then select the Group, Client, Computer, User that you want to monitor, the Content Aware Policy to be considered, and the event that will trigger the notification. The filter is designed to make finding information quick and easy.

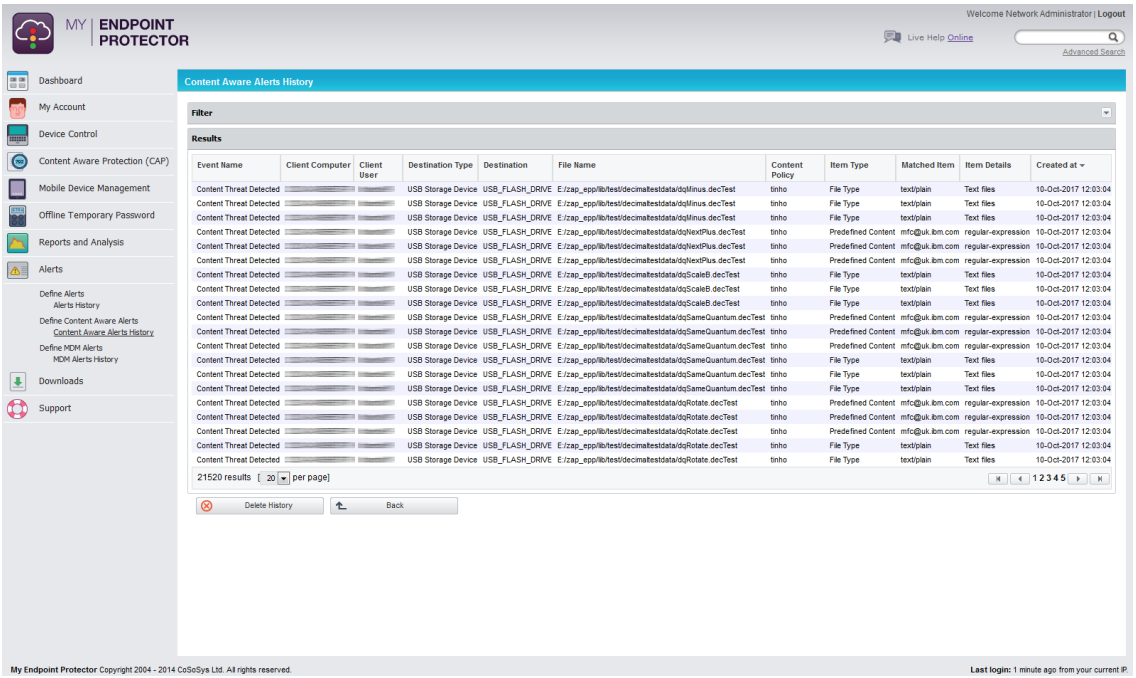
Example: if you want to be notified when a file containing credit card information is attached to an E-MAIL on one of the Financial Departments computers, you must set up an alert choosing the Financial Department as the monitored entity, the Content Aware Policy that inspects documents for that type of information and, finally, selecting the “Content Threat Detected” event from the events list.

Note!

Before creating the alert, make sure that the selected Content Aware Policy is enabled on the chosen Computer, User, Group or Department.

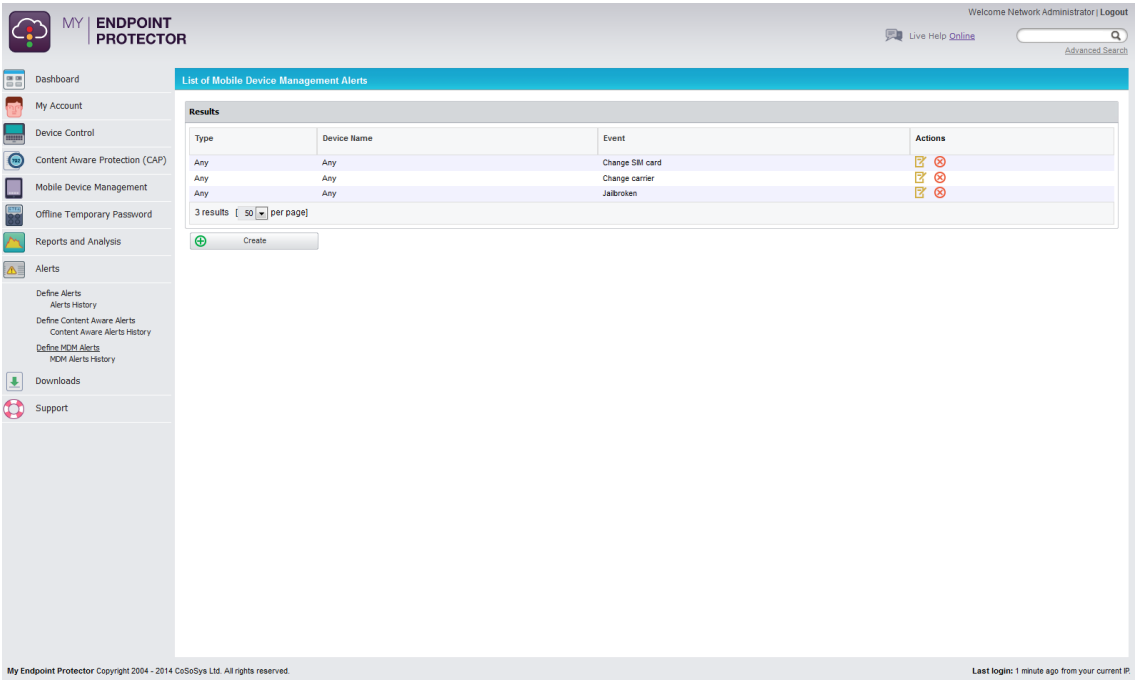
9.4. Content Aware Alerts History

A history of the content aware alerts is kept in this tab for later auditing. Each event that triggers a content aware alert will be saved here. Administrators can search for data more easily with the implemented filter, while if not needed anymore the logs can be deleted from the "Delete History" button.



9.5. Define MDM Alerts

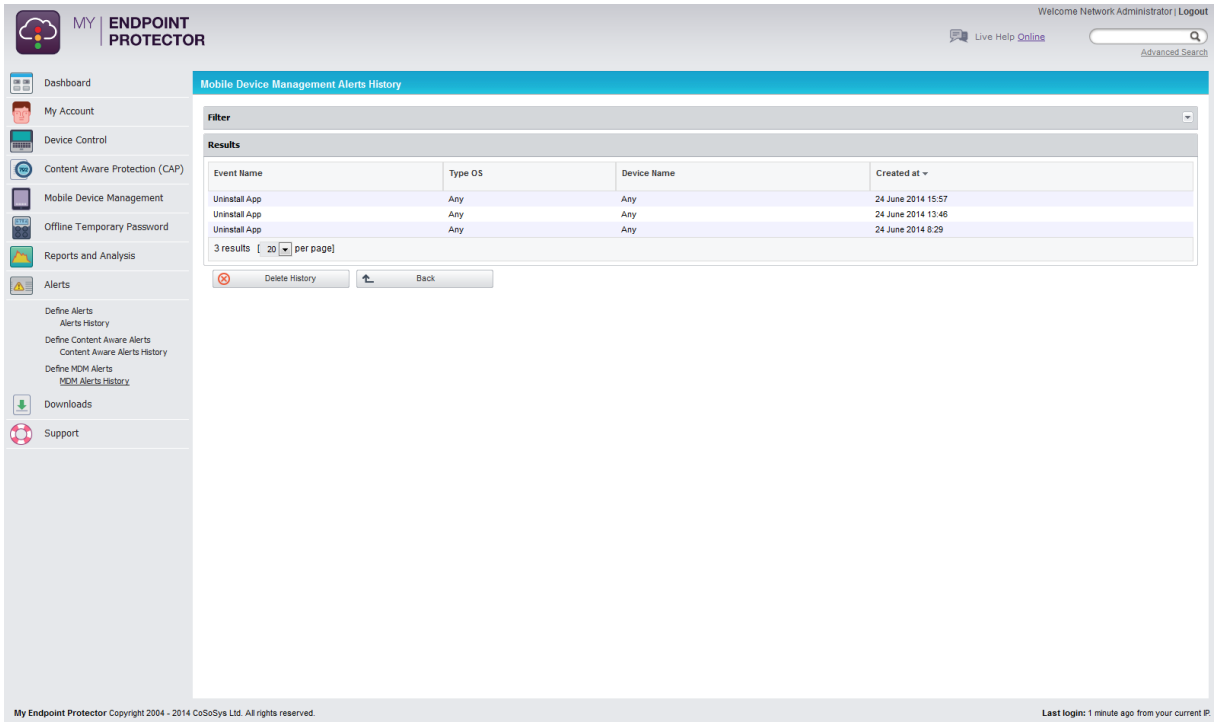
To create a new MDM alert go to the "Define MDM Alerts" tab and press the "Create" button.



Alerts can be created for IOS MDM profile removal, Android application removal, SIM card changed and carrier changed.

9.6. MDM Alerts History

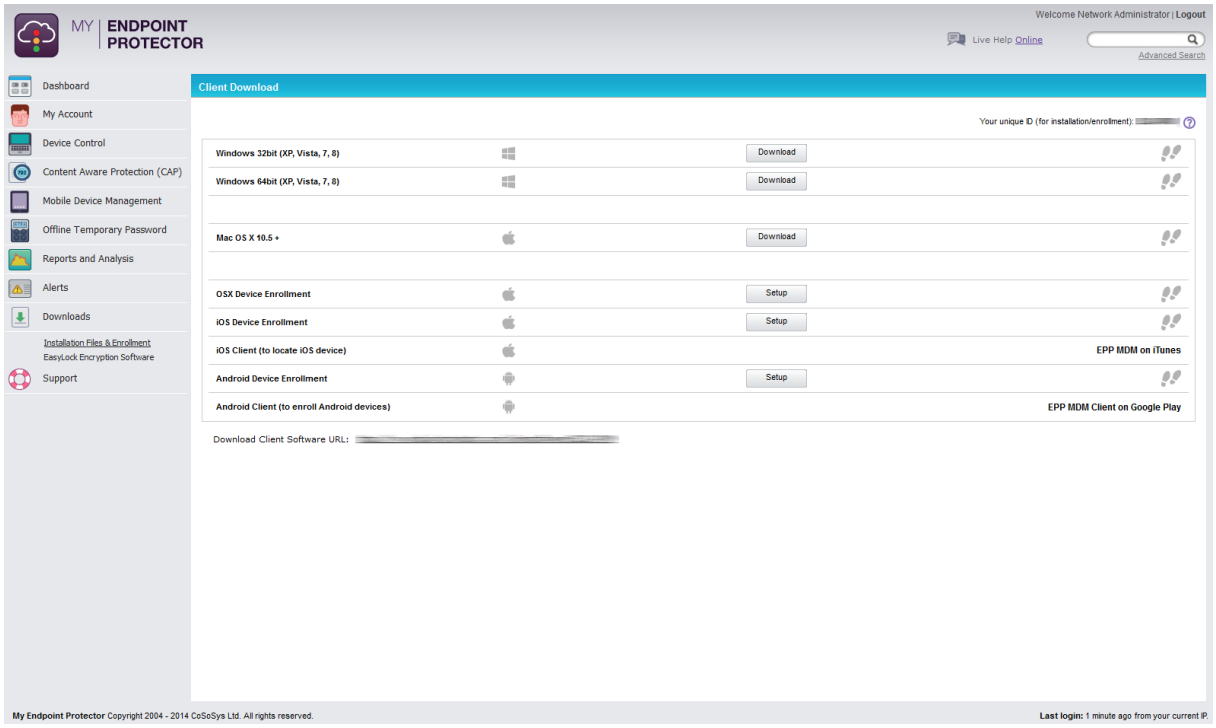
A history of the MDM alerts is kept in this tab for later auditing. Each event that triggers an MDM alert will be saved here. Administrators can search for data more easily with the implemented filter, while if not needed anymore the logs can be deleted from the "Delete History" button.



10. Downloads

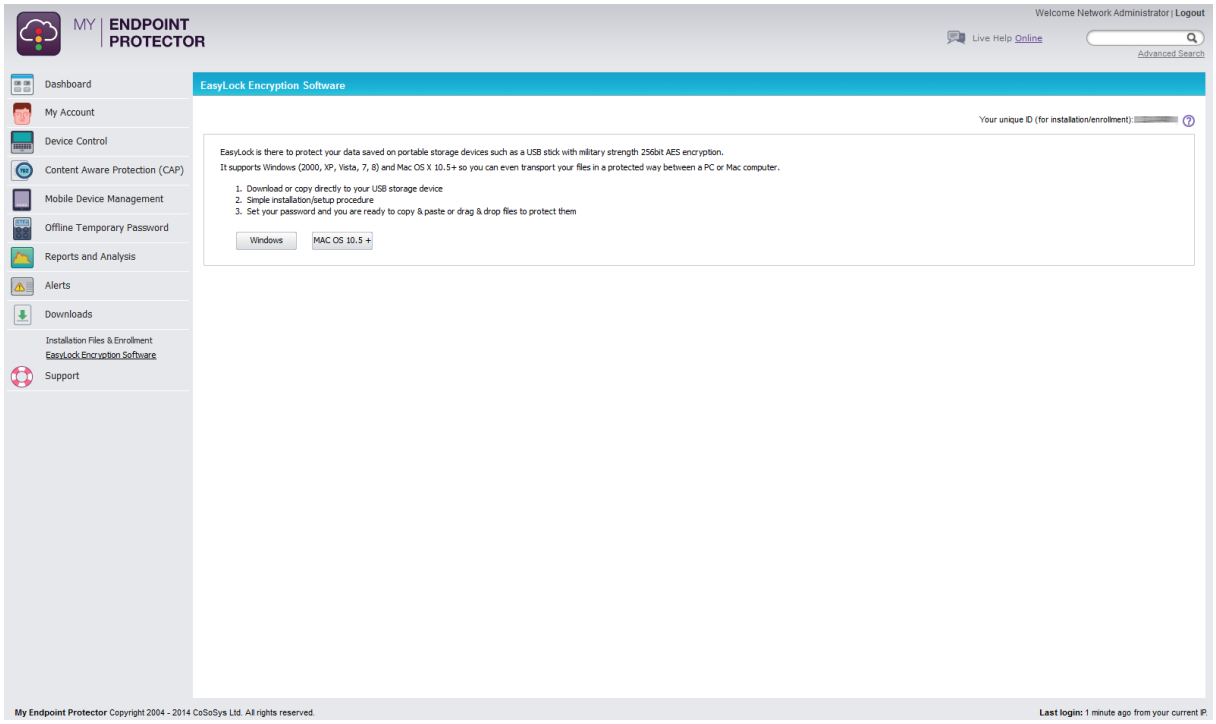
10.1. Installation Files & Enrollment

The latest Windows and MAC clients for My Endpoint Protector can be downloaded from this module.



10.2. EasyLock Encryption Software

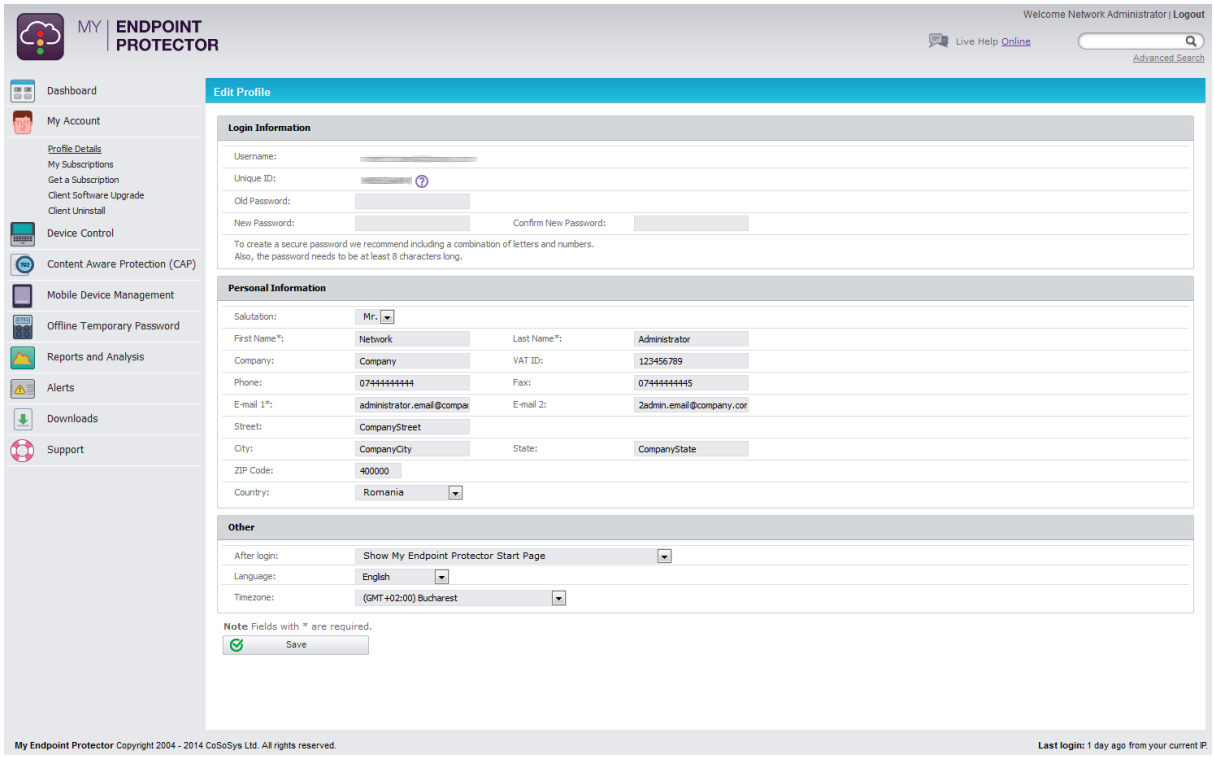
The latest Windows and MAC version of EasyLock 2 Encryption Software can be downloaded from this module.


MY ENDPOINT PROTECTOR
Welcome Network Administrator | Logout
Live Help Online
Advanced Search
Dashboard
My Account
Device Control
Content Aware Protection (CAP)
Mobile Device Management
Offline Temporary Password
Reports and Analysis
Alerts
Downloads
Installation Files & Enrollment
EasyLock Encryption Software
Support
EasyLock Encryption Software
Your unique ID (for installation/enrollment):
EasyLock is there to protect your data saved on portable storage devices such as a USB stick with military strength 256bit AES encryption.
It supports Windows (2000, XP, Vista, 7, 8) and Mac OS X 10.5+ so you can even transport your files in a protected way between a PC or Mac computer.
1. Download or copy directly to your USB storage device
2. Simple installation/setup procedure
3. Set your password and you are ready to copy & paste or drag & drop files to protect them
Windows
MAC OS 10.5 +
My Endpoint Protector Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.
Last login: 1 minute ago from your current IP.

11. My Account

11.1. Profile Details

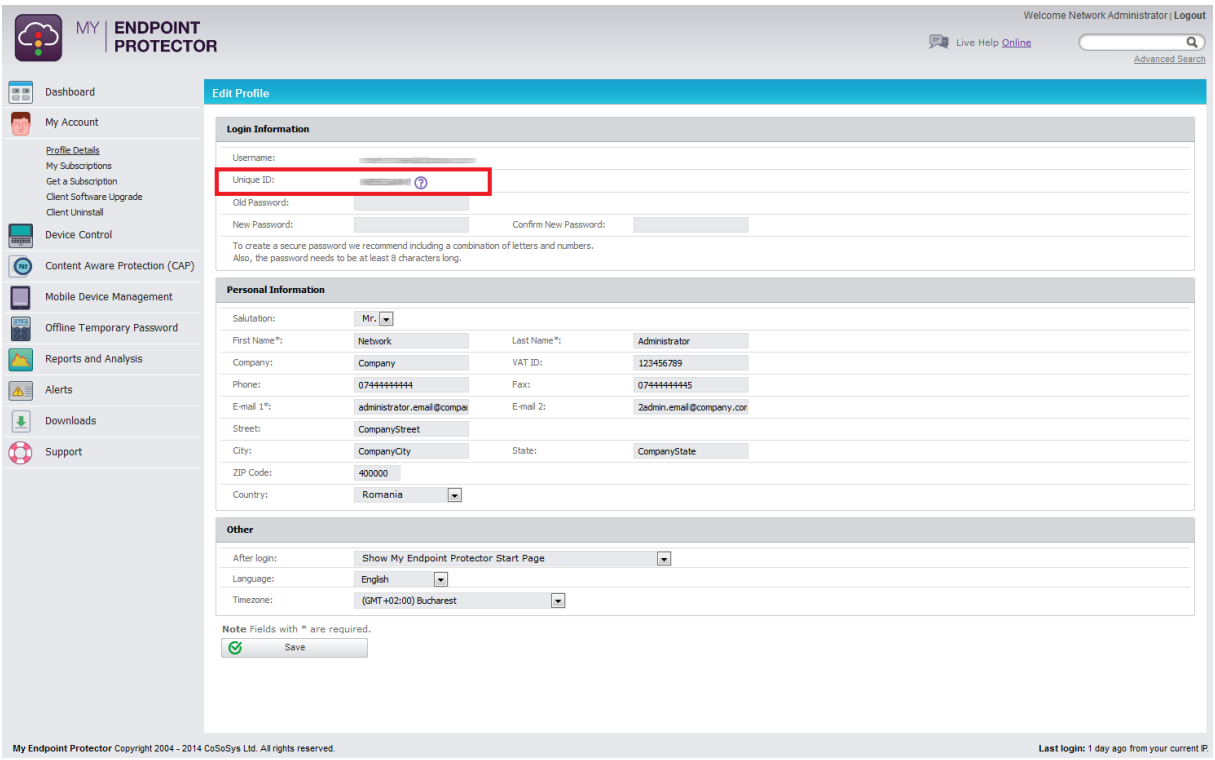
Personal information can be stored in this module. You can change this information anytime.



11.2. Unique ID

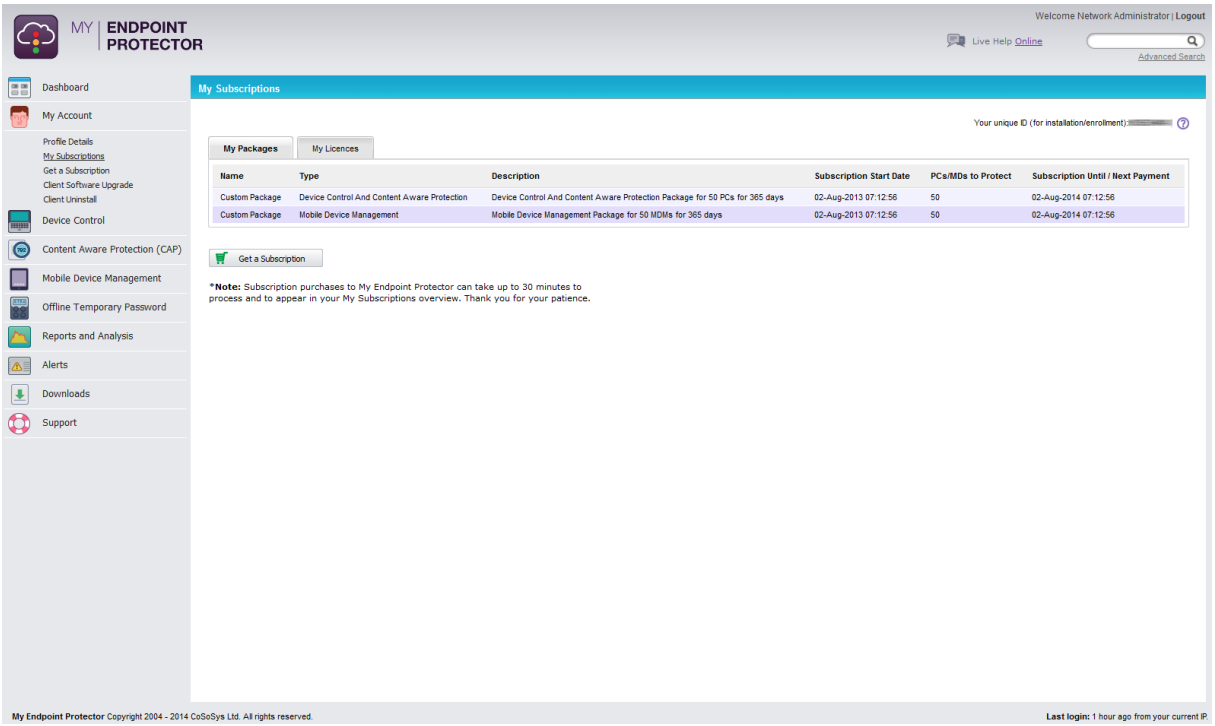
The My Endpoint Protector **Unique ID** is an important part of your account. It is mandatory you enter it when installing the My Endpoint Protector client/agent on a new computer. It is also essential when purchasing additional licenses through the E-Store.

You can find your Unique ID in the **Profile Details**, **My Subscriptions**, **Get a Subscription**, **Installation Files and Enrollment** and **Download EasyLock Software** tabs. The last two tabs can be found under the Downloads module.



11.3. My Subscriptions

My Subscriptions contains a list of your subscriptions (trial, appetizer and paid ones) with information like their type, their number and their expiration date.



Licenses can be purchased for Device Control, Device Control and Content Aware Protection and separately for Mobile Device Management.

Device Control licenses are used for registering the My Endpoint Protector Client, enabling the communication with the My Endpoint Protector Server. Once registered with a valid Endpoint license, the My Endpoint Protector Client remains active for an unlimited period of time regardless of the status of the other license types.

Content Aware Protection licenses can be purchased together with Device Control licenses. Since these licenses are purchased together they are also assigned as such to endpoints, meaning that a Computer can't take separately a DC license or CAP license, instead it will take one DC+CAP license.

Mobile Device Management licenses are used for registering Mobile Devices. The licenses are assigned when a new mobile device is enrolled.

Note!

When signing up for the first time to My Endpoint Protector you must choose either Trial license or Appetizer license as the account type. Only after creating this type of account you will be able to purchase perpetual licenses from the user interface.

11.3.1. Trial license

The trial license account type can be chosen when signing up for the first time, which upon creation will assign 10 day trial licenses for up to 50 computers and 5 mobile devices.

The trial licenses are assigned on a "first-in-first-served" basis. In case that one or more computers with assigned trial licenses are inactive for a certain interval of time, the administrator can manually release those licenses, which will automatically be reassigned to other online computers.

11.3.2. Appetizer license

The appetizer license account type can be chosen when signing up for the first time, which upon creation will assign 1 year appetizer licenses for up to 5 computers and 5 mobile devices.

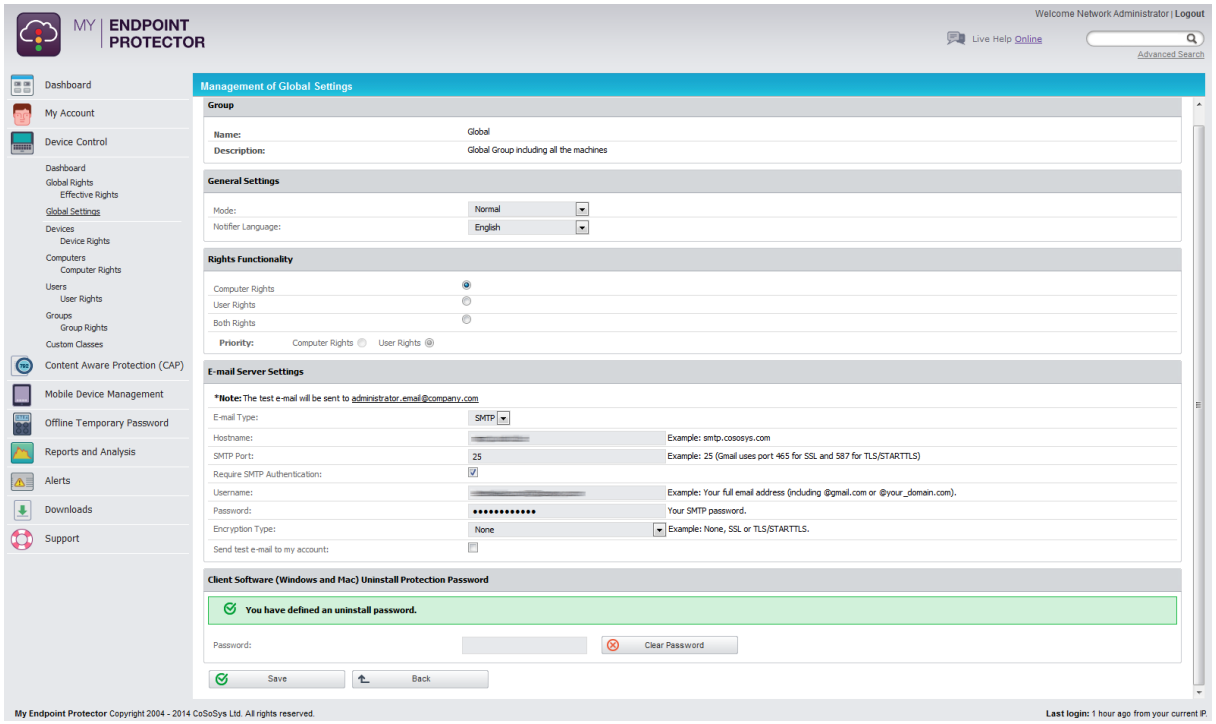
11.4. Get a Subscription

Here you can simply purchase a subscription. For that enter the number of Computers (PCs or MACs) that you want to protect and the time period for which you want the protection to cover.

11.5. Client Uninstall Protection

The Client Uninstall Protection feature protects the My Endpoint Protector Client from being uninstalled by using a password-based mechanism. The My Endpoint Protector Administrator defines this password from within the Reporting and Administration Tool of My Endpoint Protector. When somebody tries to uninstall the My Endpoint Protector Client, they will be prompted for the password. If they do not know the password, the Client removal cannot continue.

This password can be set by accessing "Device Control" – "Global Settings", entering a password in the "Client Software (Windows and Mac) Uninstall Protection Password" field and clicking on "Save". To clear the password simply click on the "Clear Password" button.



12. My EPP App for iPhone and iPad

My Endpoint Protector users can check the status of their Computers and Device use with the My EPP App for iPhone, iPad and iPod touch.

The App can be installed through iTunes (search for My EPP).

The App is available directly here:

http://ax.itunes.apple.com/us/app/my-endpoint-protector/id379244830?mt=8

13. Enforced Encryption with TrustedDevices

Protecting Data in Transit is essential to ensure no third party has access to data in case a device is lost or stolen. The Enforced Encryption solution gives administrators the possibility to protect confidential data on portable devices in case of loss or theft. If a TrustedDevice fails to get authorization from the My Endpoint Protector server, then it will not be usable.

How does it work?

Enforcing Encryption can be done by using TrustedDevices. TrustedDevices must receive authorization from the My Endpoint Protector server, otherwise they will be unusable.

There are four levels of security for TrustedDevices:

- Level 1 - Minimum security for office and personal use with a focus on software based encryption for data security. Offers companies already regulatory compliance.
  Any USB Flash Drive and most other portable storage devices can be turned into a TrustedDevice Level 1 with EasyLock Software from CoSoSys.
  No hardware upgrade is required.

- Level 2 - Medium security level with biometric data protection or advances software based data encryption.
  Requires special hardware that includes security software and that has been tested for TrustedDevice Level 2.
  Hardware is widely available in retail stores.

- Level 3 - High security level with strong hardware based encryption that is mandatory for sensitive enterprise data protection for regulatory compliance such as SOX, HIPAA, GBLA, PIPED, Basel II, DPA, or PCI

95/46/EC.
Requires special hardware that includes advanced security software and hardware based encryption and that has been tested for TrustedDevice Level 3.

- Level 4 - Maximum security for military, government and even secret agent use. Level 4 TrustedDevices include strong hardware based encryption for data protection and are independently certified (e.g. FIPS 140). These devices have successfully undergone rigorous testing for software and hardware.
  Requires special hardware that is available primarily through security focused resellers.

13.1. How a Level 1 TrustedDevice Works

User connects Device to My Endpoint Protector protected Client PC. Device is blocked by My Endpoint Protector (default action).

Device is checked for authorization.

If device is an authorized TrustedDevice Level 1, the EasyLock software on Device will automatically open.

User can transfer files via Drag & Drop in EasyLock from the PC to the TrustedDevice.

Data transferred to devices is encrypted via 256bit AES.

User cannot access the device using Windows Explorer or similar applications (e.g. Total Commander).

User does not have the possibility to copy data in unencrypted state to the TrustedDevice.

“TrustedDevice” implies that the devices offer a safe, risk-free environment to transfer sensitive data.

Administrator can audit what user, with what device, on what PC, has transferred what files.

13.2. EasyLock Software for TrustedDevices Level 1

EasyLock allows portable devices to be identified as TrustedDevices and protects data on the device with government-approved 256bit AES CBC-mode encryption. With the intuitive Drag & Drop interface, files can be quickly copied to and from the device.

To install EasyLock on an USB Flash drive one has to copy the file "EasyLock.exe" to the root folder of a partition associated with that device.

Managing TrustedDevices from EPP server console

Access to TrustedDevices can be configured from the Global Rights module of My Endpoint Protector, under Rights tab.

Access the drop-down box next to USB Storage Device and select the desired level of TrustedDevices you wish to grant access to.

EasyLock is available here:

http://www.endpointprotector.com/en/index.php/products/easylock

Purchase a license here:

http://www.endpointprotector.com/en/index.php/epp/estore

https://secure.avangate.com/order/cart.php?PRODS=1905891

14. My Endpoint Protector Client

The My Endpoint Protector Client is the application which once installed on the client Computers (PC's), communicates with the My Endpoint Protector server and blocks or allows devices to function, as well as sends out notifications in case of unauthorized access.

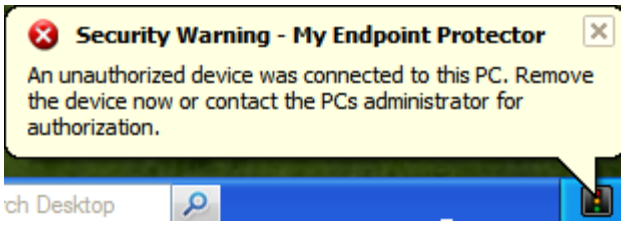
14.1. My Endpoint Protector Client Security

The My Endpoint Protector Client has a built in security system, which makes stopping the service nearly impossible.

This mechanism has been implemented to prevent the circumvention of security measures enforced by you. If somebody tries to connect unauthorized devices, they are blocked. If the individual has a bad intent to steal data from you he or she will try to circumvent your My Endpoint Protector security. With this build in security it makes this nearly impossible for any normal user.

14.2. Client Notifications (Agent)

The My Endpoint Protector Client, depending on the mode it is currently running on, will display a notification from the taskbar icon when an unauthorized device is connected to the system. Not only does it log any attempts to forcefully access to system, but it can also trigger the system's Panic mode.


Security Warning - My Endpoint Protector
An unauthorized device was connected to this PC. Remove the device now or contact the PCs administrator for authorization.
ch Desktop

14.3. Offline Functionality for My Endpoint Protector Client

The My Endpoint Protector Client will store a local event history that will be submitted and synchronized with the My Endpoint Protector Cloud Server upon next connection to the network. The client remembers the last settings and rights. If the protected PC is not connected to the internet, permissions can be given to allow devices temporary using the Offline Temporary Password feature (as described in paragraph 7.”).

14.4. DHCP / Manual IP address

My Endpoint Protector Client automatically recognizes changes in the network’s configuration and updates settings accordingly, meaning that you can keep your computer protected at the office (e.g. DHCP) and at home (e.g. manual IP address) too, without having to make any modifications.

14.5. Client Removal

14.5.1. Client Removal on Windows OS

The My Endpoint Protector Client can be uninstalled by accessing Control Panel › Add Remove Programs › Uninstall My Endpoint Protector.

The My Endpoint Protector Client cannot be uninstalled without specifying the password set by the administrator(s) in the Reporting and Administration Tool (if set).

To use this password-protect feature, please consult the “Client Uninstall Protection” paragraph.

The password sent by the My Endpoint Protector Server is hashed and stored inside the registry. If it is deleted, the uninstall process will instantly stop. Tampering with the registry value of the hash will lead to an irremovable client.

14.5.2. Client removal on MAC OS X

To uninstall the My Endpoint Protector client for Mac OS X you need to run the "remove-epp.command" script file that was provided to you in the installation package.

You can do this by double clicking the file in the "Finder".

You will be prompted for your user password with the following text: "Enter your password to perform administrative tasks:".

You need to provide your user password and then hit the "Return" key (please note that the password will not be echoed).

The password is the password that you choose when you created your user account on the MAC computer.

Important!

If your MAC user account does not have administrative privileges, un-installation is not possible.

To assure that your user password is the correct one go to the: the Accounts settings in System preferences and try to change your password.

15. Terms and Definitions

Here you can find a list of terms and definitions that are encountered throughout the user manual.

15.1. Server Related

Computers – refers to PC's, workstations, thin clients, notebooks, which have My Endpoint Protector Client installed.

File Tracing - this feature will track all data that was copied to and from prior authorized portable storage devices.

File Shadowing – this feature saves a copy of all, even deleted files that were used in connection with controlled devices on a network storage server.

Devices – refers to a list of known portable storage devices, ranging from USB storage devices to digital cameras, LTP, COM, Serial port storage devices and biometric devices.

Groups – can be groups of devices, users or computers. Grouping any of these items will significantly help the server administrators to easily manage rights and settings for them.

15.2. Client Related

Endpoint – can be a Personal Computer, a Workstation you use at the office or a Notebook. An endpoint can call and be called. It generates and terminates the information stream.

TrustedDevices – portable storage devices that carry a seal of approval from the My Endpoint Protector Server and can be used according to their level (1-4). For more information please see "Enforced Encryption with TrustedDevices" section.

Client - refers to the client user who is logged in on a computer and who facilitates the transaction of data.

Rights – applies to computers, devices, groups, users and global rights; it stands for privileges that any of these items may or may not possess.

Online computers – refers to PC's, Workstations and/or Notebooks, which have My Endpoint Protector Client installed and are currently running and are connected to the My Endpoint Protector server.

Connected devices – are devices, which are connected to online computers.

Events – are a list of actions that hold major significance in My Endpoint Protector. There are currently 17 events, which are monitored by My Endpoint Protector:

- Connected – the action of connecting a device to a computer running My Endpoint Protector Client.
- Disconnected – the action of (safely) removing a device from a computer running My Endpoint Protector Client.
- Enabled – refers to devices; the action of allowing a device access on the specified computer(s), group(s) or under the specified user(s).
- Disabled – refers to devices; the action of removing all rights from the device, making it inaccessible and therefore unusable.
- File read - a file located on a portable device was opened by a user or the file was automatically opened if the portable device was autorun by the operating system.
- File write – a file was copied onto a portable devices.
- File read-write – a file located on a portable device was opened and edited; changes were saved to the file.
- File renamed – a file located on a portable device has been renamed.
- File delete – a file located on a portable device has been deleted.

- Device TD – means that a device is registered as a TrustedDevice and has access to files accordingly.
- Device not TD – means that a device is not trusted and does not have automatic access to files.
- Delete – refers to computers, users, groups, alerts and devices; the action of removing any of these items from the list.
- Enable read-only – refers to devices; the action of allowing access to devices, but disabling the ability to write on them. User(s) can copy files from device(s), but cannot write anything onto the device.

Enable if TD Level 1-4 - refers to TrustedDevices; grants the device access if the device is a level one, two, three or four

16. Endpoint Protector Product Family

The Endpoint Protector Product family offers device control and endpoint security for any environment for home PCs or MACs, medium sized offices or even entire enterprise networks.

My Endpoint Protector is part of it and offers your home and office PCs and MACs the best solution to control the use of portable devices on your protected computers so you data cannot be copied unauthorized to unwanted devices.

Other products from the Endpoint Protector Product family are:

- Endpoint Protector Appliance (a hardware appliance device control solution for small and medium sized companies and enterprises)
- Endpoint Protector (a client - server device control solution for small and medium sized companies)
- Endpoint Protector Basic (a standalone solution to secure PCs and MACs locally. Endpoint Protector Basic has no server or online management console.

They offer **great advanced features** such as:

- File Tracing
- File Shadowing
- File Whitelisting
- AD integration
- And many more.

More information can be found here http://www.EndpointProtector.com

17. Support

In this module you can download the user manual, contact support if you need additional help, find out what's next on our TO DO list, visit our website, and more.

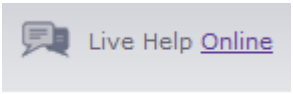
You can consult the FAQ database by following this link

http://www.endpointprotector.com/en/index.php/products/How_it_Works_My_Endpoint_Protector#

or

http://www.cososys.com/help.html

You can also chat with an endpoint security technician using the Live Help feature of My Endpoint Protector.



Even if you do not have a problem but miss some feature or just want to leave us general comment we would love to hear from you. Your input is much appreciated and we welcome any input to make computing with portable devices safe and convenient.

18. Important Notice / Disclaimer

Security safeguards, by their nature, are capable of circumvention. CoSoSys cannot, and does not, guarantee that data or devices will not be accessed by unauthorized persons, and CoSoSys disclaims any warranties to that effect to the fullest extent permitted by law.

© 2004 – 2014 CoSoSys Ltd.; Endpoint Protector Basic, EPPBasic, Endpoint Protector, My Endpoint Protector are trademarks of CoSoSys Ltd. All rights reserved. Windows is registered trademark of Microsoft Corporation. Macintosh, Mac OS X are trademarks of Apple Corporation. All other names and trademarks are property of their respective owners.